BARTON COUNTY COMMUNITY COLLEGE

HIPAA MEDICAL PRIVACY POLICY AND PROCEDURES

Documents prepared by:

BARTON COUNTY COMMUNITY COLLEGE
ORGANIZED HEALTH CARE ARRANGEMENT
HIPAA MEDICAL PRIVACY
POLICY AND PROCEDURES
TABLE OF CONTENTS

Notices of Privacy Practices

Full Version for the Barton County Community College Medical, Dental, and Prescription Plan, Barton County Community College Level II Preventive Health Benefits Plan, and Barton Community College Health Flexible Spending Account

Reminder of the Notices of Privacy Practices

Privacy Policy and Procedures

Exhibits:

1. Notices of Privacy Practices (See Tab 1 behind *Notices of Privacy Practices*)
2. Authorization For Release of Protected Health Information
3. Request For Access to Protected Health Information
4. Response to Request For Access to Protected Health Information
5. Request to Amend Protected Health Information
6. Response to Request to Amend Protected Health Information
7. Request for Accounting of Disclosures of Protected Health Information
8. Response to Request for Accounting of Disclosures of PHI
9. Request for Confidential Communications
10. Response to Request for Confidential Communications
11. Request for Restrictions to Protected Health Information
12. Response to Request for Restrictions to Protected Health Information
13. Disclosure Report Form
14. Employee Training Log
15. Employee Acknowledgment
16. Risk Analysis Worksheet
17. Breach Determination – Risk Assessment
18. Log of Breaches of Unsecured Protected Health Information ("PHI")

Miscellaneous Administrative Forms

1. Organized Health Care Arrangement Designation Form
2. Hybrid Entity Designation Form
3. Privacy Officer Designation and Acceptance Form

Table of Contents *(continued)*

4. Security Officer Designation and Acceptance Form
5. Contact Person Designation and Acceptance Form
6. Technical and Physical Safeguard Worksheet
7. HIPAA Privacy & Security Safeguards – Checklist
8. Business Associate Worksheet

Business Associate Agreement

HIPAA Medical Privacy Outline

Regulations on HIPAA Privacy and Security (2013)

Initial HIPAA Compliance Checklist

NOTICES OF PRIVACY PRACTICES

Barton County Community College Organized Health Care Arrangement

Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The Barton County Community College Medical, Dental, and Prescription Plan, Barton County Community College Level II Preventive Health Benefits Plan, and Barton Community College Health Flexible Spending Account have, for purposes of complying with the HIPAA medical privacy regulations, formed an "organized health care arrangement" (the "OHCA"). An OHCA is authorized to issue a joint Notice of Privacy Practices and develop one set of policies and procedures applicable to all group health plans that are members of the OHCA. Group health plans that are members of an OHCA are authorized to share protected health information with each other as necessary to carry out treatment, payment or health care operations and as necessary to manage and operate the organized health care arrangement.

This Notice describes the legal obligations of the OHCA and your legal rights regarding your protected health information ("PHI") held by the OHCA under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The OHCA is required by law to maintain the privacy of PHI and to provide you with this Notice of its legal duties and privacy practices with respect to PHI. This Notice describes the circumstances under which your PHI may be used or disclosed by the OHCA to carry out treatment, payment, or health care operations or for any other purpose that is permitted or required by law. The privacy laws of a particular state or other federal laws might impose a more stringent privacy standard. If these more stringent laws apply and are not superseded by federal preemption rules under the Employee Retirement Income Security Act of 1974 ("ERISA"), the OHCA will comply with the more stringent law.

In general, "protected health information" or "PHI" is individually identifiable information, including demographic information, collected from you or created or received by a health care provider, a health care clearinghouse, a health plan, including the OHCA, or by Barton County Community College on behalf of the OHCA, that relates to the following:

(1) Your past, present or future physical or mental health or condition;
(2) The provision of health care to you; or
(3) Your past, present or future payment for the provision of health care to you.

I. The OHCA's Responsibilities Regarding PHI

Each group health plan listed above, that is a member of the OHCA, is considered "self-funded." The OHCA, on behalf of its individual members, is required by law to:

- Protect and maintain the privacy of your PHI in accordance with HIPAA;
- Provide you with certain rights relating to your PHI;
- Notify you following a breach of your unsecured PHI;
- Prepare and maintain this Notice of our legal duties and privacy practices with respect to your PHI;
- Provide a copy of this Notice to you;

- Provide a copy of this Notice to an individual at the time he or she enters a group health plan that is a member of the OHCA;
- Within 60 days of a material modification of this Notice, provide a copy of the revised Notice to you;
- No less frequently than every three years, notify all individuals enrolled in a group health plan that is a member of the OHCA of the availability of this Notice and how to obtain a copy (i.e., send out a Reminder Notice); and
- Follow the terms of the Notice that is currently in effect.

II. How the OHCA May Use and/or Disclose Your PHI

The following categories describe different ways that the OHCA may use and/or disclose your PHI. Not every use or disclosure in a category will be listed. However, all the ways the OHCA is permitted to use and disclose your PHI will fall within one of the categories. However, records about any substance use disorder treatment ("SUD") you have received from a federally-assisted substance use disorder treatment program are protected by federal law, 42 CFR Part 2, and are subject to additional privacy safeguards. Please note that information disclosed by the OHCA to an outside person or entity as described in this Notice may be subject to redisclosure by the recipient and might no longer be protected by the HIPAA Privacy Rule.

For Treatment
• The OHCA may disclose your PHI to your health care provider for its provision, coordination or management of your health care and related services. For example, the OHCA may disclose your PHI to your health care provider for purposes of coordinating your health care with the OHCA or referring you to another provider for care. • However, if your PHI includes SUD records, the OHCA will not disclose those records for treatment purposes without your written consent, except as specifically permitted or required by law.
For Payment
• The OHCA may use and disclose your PHI to determine eligibility for benefits under a group health plan that is a member of the OHCA, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under a group health plan that is a member of the OHCA, or to coordinate coverage of a group health plan that is a member of the OHCA. For example, the OHCA may tell your health care provider about your medical history to determine whether a particular treatment is medically necessary or to determine whether the plan that is part of the OHCA will cover the treatment. • The OHCA may also share medical information with a utilization review or pre-certification service provider. Likewise, the OHCA may share PHI with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments. • In addition, an explanation of benefits ("EOB"), which may contain information such as the name of the individual receiving treatment, the name of the health care provider, the date medical care is received, the amount charged for medical care, and the amount paid for medical care, may be sent to the individual through whom

coverage is provided. For example, a covered employee may receive an EOB disclosing the information listed above with respect to his or her spouse or any dependents covered through such employee.

- This disclosure for payment purposes is subject to an individual's right to request confidential communications as explained below. However, records will not be used or disclosed for payment purposes without your written consent, except as specifically allowed or required by law.

For Health Care Operations

- The OHCA may use and disclose your PHI for OHCA operations. These uses and disclosures are necessary to run the OHCA. For example, we may use PHI in connection with conducting quality assessment and improvement activities; underwriting, premium rating, and other activities relating to coverage under a group health plan that is part of the OHCA (excluding genetic information for underwriting purposes); submitting claims for stop-loss (or excess loss) coverage; conducting or arranging for medical review, legal services, audit services, and fraud and abuse detection programs; business management and development; and OHCA administration.
- However, the OHCA will not use or disclose any SUD records for health care operations without your written consent, except as specifically permitted by law.

As Required By Law

- The OHCA will disclose medical information about you when required to do so by federal, state or local law. For example, the OHCA may disclose your PHI when required by national security laws or public health disclosure laws.
- However, if a disclosure required by another law involves SUD records, the OHCA will only make such a disclosure in compliance with the stricter requirements of 42 CFR Part 2, such as with your written consent or a court order that meets Part 2's stricter criteria.

To Avert a Serious Threat to Health or Safety

- The OHCA may use and disclose your PHI when necessary to prevent a serious threat to the health and safety of yourself, the public, or another person. Any disclosure would only be to someone able to help prevent or reduce the threat. For example, the OHCA may disclose medical information about you in a proceeding regarding the licensure of a physician.
- However, SUD records will only be disclosed to avert such a serious threat as allowed by 42 CFR Part 2, which generally means your written consent or a specific court order is required for any disclosure of those records.

To a Business Associate

- The OHCA may enter into contracts with individuals or entities known as Business Associates ("BA") to perform various functions or services on behalf of the OHCA. To the extent necessary to perform these functions or services, BAs may receive from the OHCA, create from information provided from the OHCA, maintain, use, and/or disclose your PHI, but only after they agree in writing with the OHCA or the member of the OHCA to which the information relates to implement and follow appropriate safeguards regarding your PHI. For example, the OHCA may disclose your PHI to a BA to administer claims or to provide support services, such as utilization management, pharmacy benefit management, or subrogation.

- However, any SUD records will only be shared with a BA in compliance with 42 CFR Part 2, for example, pursuant to your written consent or under a qualified service agreement expressly permitted by law.

To the Plan Sponsor

- The OHCA may disclose your PHI to certain employees of the Plan Sponsor for purposes of administering the OHCA. However, those employees will use or disclose the information received only as necessary to perform OHCA administrative functions or as otherwise required by HIPAA, unless you have authorized further disclosures.
- Your PHI may not be used for employment purposes without your specific authorization. In addition, if any information to be shared with the Plan Sponsor includes SUD records, the OHCA will not disclose those records to the Plan Sponsor without your written consent, unless specifically permitted by applicable law.

Military and Veterans

- If you are a member of the armed forces, the OHCA may disclose your PHI as required by military command authorities. We may also release PHI about foreign military personnel to the appropriate foreign military authority.
- However, SUD records will not be disclosed to military authorities without your written consent or a specific authorization as required by 42 CFR Part 2.

Workers' Compensation

- The OHCA may disclose PHI about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.
- However, SUD records will not be disclosed for workers' compensation purposes without your written consent or a court order that meets the requirements of 42 CFR Part 2.

Organ and Tissue Donation

- If you are an organ donor, the OHCA may disclose PHI about you to organizations that handle organ donor procurement or transplantation, as necessary to facilitate organ or tissue donation and transplantation.
- However, the OHCA will not disclose any SUD records for organ or tissue donation purposes without your written consent, except as specifically permitted by federal law.

Public Health Risks

- The OHCA may disclose your PHI for public health activities including, but not limited to: prevent or control disease, injury or disability and to report births and deaths.
- However, any information from SUD records will only be disclosed for the public health purposes listed above if permitted by 42 CFR Part 2. For example, Part 2 regulations allow reporting of suspected child abuse or neglect to appropriate authorities, but other public health disclosures (such as disease exposure notifications) would require your written consent or a court order.

Health Oversight Activities

- The OHCA may disclose your PHI to a health oversight agency for activities authorized by law.
- However, any SUD records will only be disclosed to oversight agencies if permitted by 42 CFR Part 2 (such as for certain audits or evaluations expressly allowed under Part 2); otherwise, your written consent or a Part 2-compliant court order would be required before disclosing such records.

Coroners, Medical Examiners and Funeral Directors
• The OHCA may disclose your PHI to a coroner or medical examiner. The OHCA may also disclose PHI to funeral directors as necessary to carry out their duties. • However, the OHCA will not disclose SUD records or related information to coroners, medical examiners, or funeral directors without appropriate patient consent or a court order, as required by law.
National Security and Intelligence Activities
• The OHCA may disclose your PHI to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law. • However, SUD records will not be disclosed for national security or intelligence purposes without your written consent or a specific authorization expressly permitting such disclosure under 42 CFR Part 2.
Inmates
• If you are an inmate of a correctional institution or under the custody of a law enforcement official, the OHCA may disclose your PHI to the correctional institution or law enforcement official. This release would be necessary: o for the institution to provide you with health care; o to protect your health and safety or the health and safety of others; or o for the safety and security of the correctional institution. • However, SUD records will not be disclosed to a correctional institution or law enforcement custodian without your written consent or a court order that meets the requirements under 42 CFR Part 2.
Research
• The OHCA may disclose your PHI to researchers when (1) all individual identifying information has been removed; or (2) when an institutional review board or privacy board has reviewed and approved the research proposal, and has established protocols to ensure the privacy of the requested information. • However, if any requested information includes SUD records, the OHCA will only disclose such records for research purposes as permitted by 42 CFR Part 2 (for example, pursuant to your written consent or under an Institutional Review Board-approved protocol that meets Part 2's requirements).

III. Circumstances under Which the OHCA Must Disclose Your PHI

The OHCA is required by law to make disclosures of your PHI in the following circumstances:

Lawsuits and Disputes
• If you are involved in a lawsuit or a dispute, the OHCA may disclose your PHI in response to a court or administrative order. The OHCA may also disclose your PHI in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested. • However, any SUD records about you that are protected under 42 CFR Part 2 will not be disclosed for these purposes unless you have provided specific written consent or a court order is obtained that complies with the requirements of 42 CFR Part 2. Federal

law prohibits the OHCA from using or disclosing SUD records, or testimony relaying the content of such records, in any civil, criminal, administrative, or legislative proceeding against you, unless based on your written consent or a court order issued after you (or the record holder) have been given notice and an opportunity to be heard.

Law Enforcement

- The OHCA may disclose your PHI if asked to do so by law enforcement in certain scenarios, including, without limitation in response to a court order, subpoena, warrant, summons or similar process or to identify or locate a suspect, fugitive, material witness, or missing person.
- Note: SUD records have additional protections as noted above and generally may not be disclosed to law enforcement without your written consent or a qualifying court order.

In Connection with Government Audits

- The OHCA is required to disclose your PHI to the Secretary of the United States Department of Health and Human Services when the Secretary is investigating or determining our compliance with HIPAA.
- However, if any information requested in such an audit includes SUD records, the OHCA will only disclose those records as allowed by 42 CFR Part 2 (for example, as part of an officially authorized Part 2 program audit/evaluation or pursuant to a court order).

Disclosures to You

- When you request, the OHCA is required to disclose to you the portion of your PHI that contains medical records, billing records, and any other records used to make decisions regarding your health care benefits.
- The OHCA is also required, when requested, to provide you with an accounting of most disclosures of your PHI where the disclosure was for reasons other than for payment, treatment or health care operations, and where the disclosure was not pursuant to your written authorization.

IV. Other Uses of PHI

Except where specifically allowed by federal law, the use and disclosure of psychotherapy notes, use and disclosure of PHI for marketing purposes, and any disclosure that constitutes a sale of PHI will be made only pursuant to your written authorization. Other uses and disclosures of your PHI not otherwise described in this Notice or the laws that apply to the OHCA will be made only with your written permission. If you give the OHCA permission to use or disclose your PHI, you may revoke that permission, in writing, at any time. If you revoke your permission, the OHCA will no longer use or disclose your PHI for the reasons covered by your written authorization. However, this will not affect any disclosures that have already been made with your permission.

V. Your Rights Regarding Your PHI

You have the following rights regarding medical information maintained by the OHCA about you:

Right to Inspect and Copy

- You have the right to inspect and copy certain PHI that may be used to make decisions about your benefits under a group health plan that is a member of the OHCA. You must submit your request in writing to the Contact Person.

- The OHCA has prepared and will provide to you upon request a "Request for Access to PHI" form that may be used by you for this purpose. To request a copy of this form, please contact the Contact Person. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request.
- In very limited circumstances, the OHCA may deny your request to inspect and copy PHI that may be used to make decisions about your benefits under a group health plan that is a member of the OHCA.
- If you are denied access to your PHI that may be used to make decisions about your benefits under a group health plan that is a member of the OHCA, you may request that the denial be reviewed by submitting a written request to the Contact Person.

Right to Amend

- If you feel that PHI the OHCA has about you is incorrect or incomplete, you may ask the OHCA to amend the information. You have the right to request an amendment for as long as the information is kept by or for the OHCA. To request an amendment, your request must be made in writing and submitted to the Contact Person.
- The OHCA has prepared and will provide to you upon request a "Request to Amend PHI" form that may be used by you for this purpose. To request a copy of this form, please contact the Contact Person. The OHCA may deny your request for an amendment if it is not in writing or does not include a reason to support the request.
- In addition, the OHCA may deny your request if you ask the OHCA to amend information that:
    - Is not part of the medical information kept by or for the OHCA;
    - Was not created by the OHCA, unless the person or entity that created the information is no longer available to make the amendment;
    - Is not part of the information which you would be permitted to inspect and copy; or
    - Is accurate and complete.
- If the OHCA denies your request, you have the right to file a statement of disagreement with the OHCA, and any future disclosures of the disputed information will include your statement.

Right to an Accounting of Disclosures

- You have the right to request an accounting of certain disclosures of your PHI. The accounting will not include:
    - Disclosures for purposes of treatment, payment, or health care operations, unless it involves a disclosure of an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized healthcare clinicians and staff;
    - Disclosures made to you;
    - Disclosures made pursuant to your authorization;
    - Disclosures made to friends or family in your presence or because of an emergency;
    - Disclosures for national security purposes; and
    - Disclosures incidental to otherwise permissible disclosures.
- To request this list or accounting of disclosures, you must submit your request in writing to the Contact Person.

- The OHCA has prepared and will provide to you upon request a "Request for Accounting of Disclosures of PHI" form that may be used by you for this purpose. To request a copy of this form, please contact the Contact Person. Your request must state a time period, which may not be longer than six years (or three years in the case of disclosures involving electronic health records, as described above) and may not include dates before the date on which the OHCA was established.
- Your request should indicate in what form you want the list (for example, paper or electronic). The first list you request within a 12-month period will be free. For additional lists, the OHCA may charge you for the cost of providing the list. The OHCA will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Additional Accounting Rights for SUD Records

- If the OHCA maintains any SUD records about you that are protected under 42 CFR Part 2, you have the right to request an accounting of all disclosures of those records made by the OHCA within the past three years (regardless of the purpose of the disclosure). This includes disclosures made for treatment, payment, or health care operations pursuant to your prior written consent, as well as any other disclosures made with your consent or as otherwise permitted by law.

Right to Request Restrictions

- You have the right to request a restriction or limitation on your PHI that the OHCA uses or discloses about you for treatment, payment or health care operations.
- You also have the right to request a limit on your PHI disclosed by the OHCA to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that the OHCA not use or disclose information about a surgery you had. The OHCA is not required to agree to your request.
- However, if your request relates to restricting the disclosure to another health plan of your PHI pertaining solely to a health care item or service for which the health care provider has been paid out-of-pocket in full and where the purpose of the disclosure would have been for carrying out payment or health care operations, the OHCA must agree to your request.
- To request any restrictions, you must make your request in writing to the Contact Person. The OHCA has prepared and will provide to you upon request a "Request for Restrictions to PHI" form that may be used by you for this purpose. To request a copy of this form, please contact the Contact Person. In your request, you must tell the OHCA:
    - What information you want to limit;
    - Whether you want to limit the OHCA's use, disclosure or both; and
    - To whom you want the limits to apply, for example, disclosures to your spouse.

Additional Rights to Request Restrictions for SUD Records

- If you have previously given written consent allowing the OHCA to use or disclose your SUD records for treatment, payment, or health care operations, you retain the right to request that the OHCA restrict any further use or disclosure of those records.
- The OHCA is not required to agree to such a request (except as noted above for services paid in full out-of-pocket), but we will consider any requested restriction and abide by it if we agree.

Right to Request Confidential Communications
• You have the right to request that the OHCA communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that the OHCA only contact you at work or by mail. • To request confidential communications, you must make your request in writing to the Contact Person. The OHCA has prepared and will provide to you upon request a "Request for Confidential Communications" form that may be used by you for this purpose. To request a copy of this form, please contact the Contact Person. • Generally, the OHCA is not obligated to grant your request for confidential communications unless you provide information establishing that disclosure of all or part of your PHI in a manner or at a location other than that requested could endanger you and the request is reasonable. Your request must specify how or where you wish to be contacted.
Right to Be Notified Following a Breach of Unsecured PHI
• The OHCA is required by law to notify you in the event of a breach of your unsecured PHI.
Right to Opt Out of Fundraising Communications
• You have the right to opt out of receiving fundraising communications from the OHCA, in the event that the OHCA engages in such communications. • If the OHCA ever intends to use or disclose any of your SUD records information for fundraising purposes, you will first be provided a clear and conspicuous opportunity to elect not to receive such fundraising communications.
Prohibition on Use or Disclosure of Genetic Information
• The OHCA is prohibited from using or disclosing PHI that relates to your genetic information for underwriting purposes.
Right to Obtain Electronic Copies of PHI
• You have the right to obtain electronic copies of your PHI if maintained in a designated record set. • You may request a specific format to receive the electronic PHI and the OHCA will comply with such request if feasible. • You may be charged a reasonable cost-based fee for the electronic PHI.
Right to Request Paper Copy of This Notice
• You have the right to a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. • To obtain a paper copy of this Notice, please contact the Contact Person.

VI. Effective Date

This Notice is effective February 16, 2026.

VII. Changes to this Notice

The OHCA reserves the right to change this Notice. The OHCA reserves the right to make the revised or changed notice effective for PHI that the OHCA already has about you as well as any information the OHCA creates or receives in the future. The Plan will distribute the revised notice in accordance with 45 C.F.R. 164.520 and the Plan's past practices.

VIII. Contact Person

The OHCA's Contact Person is:
Benefit Specialist
245 NE 30
Great Bend, KS 67530
(620) 792-9235

IX. Complaints

If you believe that your privacy rights have been violated, you may file a complaint with the OHCA and with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the OHCA, contact the Contact Person listed above. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with us.

Barton County Community College Organized Health Care Arrangement

– Reminder of the Notice of Privacy Practices –

This is a Reminder that the Notice of Privacy Practices is available to you upon request. This Notice describes how medical information about you may be used and disclosed by the Barton County Community College Organized Health Care Arrangement (the "OHCA"), which consists of the Barton County Community College Medical, Dental, and Prescription Plan, Barton County Community College Level II Preventive Health Benefits Plan, and Barton Community College Health Flexible Spending Account, to carry out treatment, payment or health care operations or for any other purpose that is permitted or required by law. The Notice further describes your legal rights regarding your protected health information held by the OHCA under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and how you can get access to this information.

If you would like to receive a copy of the Notice of Privacy Practices, please contact the OHCA's Contact Person. The OHCA's Contact Person is the Benefit Specialist and may be contacted at 245 NE 30, Great Bend, Kansas 67530, (620) 792-9235.

HIPAA MEDICAL PRIVACY
POLICY AND PROCEDURES

Barton County Community College Organized Health Care Arrangement
HIPAA Privacy Policy and Procedures

Table of Contents

Introduction 1

A. Protected Health Information 1

B. Authorized Employees 1

C. Prohibited Action 2

D. Privacy Officer / Contact Person / Security Officer 2

I. The Notice of Privacy Practices 2

II. Use and Disclosure of Protected Health Information 4

A. Use and Disclosure for Treatment, Payment & Health Care Operations 4

B. Other Permitted Uses and Disclosures of Protected Health Information 5

1. Disclosures to Plan Sponsor 5

2. Disclosures to Business Associates 5

3. Disclosures for Legal and Public Policy Purposes 5

C. Mandatory Disclosures of Protected Health Information 6

1. Request Made by Individual 6

2. Request Made by Department of Health and Human Services 6

D. Use and Disclosures Pursuant to Authorizations 6

III. Individual Rights 7

A. Right of Access to Protected Health Information 7

B. Right to Request Amendment to Protected Health Information 9

C. Right to Request Accounting 10

D. Right to Request Alternative Communications 12

E. Right to Request Restrictions 13

IV. Administrative Provisions and Safeguards 14

A. Documentation 14

B. Verification of Identity 14

1. Request Made by Individual 14

2. Request Made by Parent of a Minor Child 15

3. Request Made by Personal Representative 15

4. Request Made by Public Official 15

5. Request Made by Spouse, Family Member or Friend 16

C. Record Storage and Access 16

1. Physical Safeguards 17

2. Technical Safeguards 17

3. Disposal 17

D. Minimum Necessary Standard 17

E. Mitigation of Inadvertent Disclosures 19

F. Employee Training 19

1. Existing Employee Training 20

2. New Employee Training 20

G. Sanctions for Violations of Policies and Procedures 20

H. Complaints 20

V. Electronic Security 21

A. Risk Analysis 21

B. Plan Document 22

C. Disclosures of Electronic PHI to Business Associates 23

D. Documentation 23

VI. Breach Notifications 24

A. Definitions of Breach / Unsecured PHI 24

B. Breach Determination and Risk Analysis 24

1. Breaches by a Business Associate 24

2. Breaches by the OHCA 25

C. Breach Notifications 25

1. Individuals 25

2. Media 26

3. HHS 26

D. Law Enforcement Delay 26

Exhibits

Notices of Privacy Practices

1. Notices of Privacy Practices (including the Reminder Notice) 1

Privacy Policy and Procedures

2. Authorization for Release of Protected Health Information 2
3. Request for Access to Protected Health Information 3
4. Response to Request for Access to Protected Health Information 4
5. Request to Amend Protected Health Information 5
6. Response to Request to Amend Protected Health Information 6
7. Request for Accounting of Disclosures of Protected Health Information 7
8. Response to Request for Accounting of Disclosures of Protected Health Information 8
9. Request for Confidential Communications 9
10. Response to Request for Confidential Communications 10
11. Request for Restrictions to Protected Health Information 11
12. Response to Request for Restrictions to Protected Health Information 12
13. Disclosure Report Form 13
14. Employee Training Log 14
15. Employee Acknowledgment 15
16. Security Risk Analysis Worksheet 16
17. Breach Determination - Risk Assessment 17
18. Log of Breaches of Unsecured PHI 18

Barton County Community College Organized Health Care Arrangement

HIPAA Privacy Policy and Procedures

Introduction

Barton County Community College (the "Company") sponsors the Barton County Community College Organized Health Care Arrangement (the "OHCA"). The OHCA consists of the Barton County Community College Medical, Dental, and Prescription Plan, Barton County Community College Level II Preventive Health Benefits Plan, and Barton Community College Health Flexible Spending Account. An organized health care arrangement ("OHCA") is authorized to issue a joint Notice of Privacy Practices and develop one set of policies and procedures applicable to all group health plans that are members of the OHCA. Group health plans that are members of an OHCA are authorized to share protected health information with each other as necessary to carry out treatment, payment or health care operations and as necessary to manage and operate the organized health care arrangement. This policy sets forth the situations in which the Company, through its employees and other agents, may obtain *protected health information* from the OHCA and the procedures that must be followed if such information is obtained.

A. "Protected Health Information"

The term "*protected health information*" means information that relates to:

(1) the past, present, or future physical or mental health or condition of an individual;

(2) the provision of health care to an individual; or

(3) the past, present, or future payment for the provision of health care to an individual.

Additionally, in order for that information to constitute *protected health information*, it must either identify the individual or else there must be a reasonable basis to believe the information can be used to identify the individual. *Protected health information* includes information that relates to persons who are both living and deceased.

B. "Authorized Employees"

It is the policy of the Company and the OHCA to comply fully with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as set forth in the regulations issued by the Department of Health & Human Services ("HHS"). To that end, access to *protected health information* shall be strictly limited to the following employees of the Company (referred to herein as "Authorized Employees"):

VP of Administration
Director of Human Resources
Benefit Specialist

In addition to the Authorized Employees listed above, upon the occurrence of an unusual and unanticipated event, for a limited time and for a limited purpose, certain employees may have access to protected health information where such access is necessary to complete one of their job functions. For example, it may be necessary for a member of the

information technology ("IT") staff to access a database containing protected health information where there is a computer virus or similar problem, a defect in hardware, or other system failure. If such access is required by someone not listed above, the Privacy Officer will ensure that such individual's access to protected health information is limited in scope and time and that such individual is appropriately trained and complies with these policies and procedures. The Privacy Officer shall identify in writing at the time of the unanticipated and unforeseeable event the designation of the individual (by name, job title or other appropriate means) who may temporarily have access to protected health information.

Authorized Employees may use and disclose *protected health information* for plan administrative functions, and they may disclose *protected health information* to other Authorized Employees for plan administrative functions (but the disclosure must be limited to the minimum amount necessary to perform the plan administrative function).

Authorized Employees may not disclose *protected health information* to other employees (other than Authorized Employees) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy.

C. Prohibited Actions

No employee of the company, including Authorized Employees, may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

D. Privacy Officer / Contact Person / Security Officer

The Privacy Officer is the VP of Administration. The Privacy Officer is responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Company's use and disclosure procedures. In addition, the Privacy Officer shall have the specific responsibilities set forth in this Policy.

The Contact Person is the Benefit Specialist. The Contact Person will answer questions and provide information about the OHCA's privacy policies and procedures. The Contact Person will also be responsible for the specific duties and responsibilities set forth in this Policy.

The Security Officer is the VP of Administration. The Security Officer is responsible for ensuring the confidentiality, integrity, and availability of all electronic *protected health information* that the OHCA creates, receives, maintains, or transmits.

I. The Notice of Privacy Practices

The Privacy Officer shall prepare and maintain a Notice of Privacy Practices ("Notice") describing the legal duties and privacy practices of the OHCA (or the individual plans which comprise the OHCA) with respect to the protected health information. A copy of the OHCA's current Notice(s) (or a copy of the OHCA member-plan's current Notice) shall be attached to

this Policy as Exhibit 1. A copy of the current Privacy Notice(s) as well as a copy of any prior versions of the Privacy Notice(s) shall be retained in accordance with the OHCA's "Documentation" policy and procedure (see Section IV. A. below).

The Contact Person shall provide a copy of the Privacy Notice to all employees who are enrolled in a group health plan that is part of the OHCA at the time they become covered under the group health plan.

If the Privacy Notice is modified or revised, a copy of the modified or revised Notice shall be provided to all employees enrolled in a plan that is part of the OHCA within 60 days of the modification or revision. The Contact Person shall also provide a copy of the current Privacy Notice upon request to a covered employee or to a person, such as a spouse or dependent, who is covered through the employee. Finally, on an annual basis, the Contact Person shall provide all covered employees, who have already received the full Privacy Notice, a Reminder Notice, informing covered employees that a Privacy Notice is available upon request. The Reminder Notice is found behind Exhibit 1. The methods of delivery are summarized in the table below.

Delivery of the Notice for the Barton County Community College Organized Health Care Arrangement:

Depending on the distribution event, the Privacy Notice will be distributed according to the table below. There are check marks in the columns which indicate a method of delivering the Privacy Notice. If one method of delivery is preferred over another, the methods will be ranked in the table below with numbers, "1" being the most preferred delivery method.

		Distribution Events for the Barton County Community College Organized Health Care Arrangement			
		Newly Covered Employee (e.g. new hires)	**Material Modification or Revision to Notice**	**Request from Participant**	**Reminder Notice**
Distribution Methods	**First Class Mail**	X	X	X	
	Hand-Delivery	X	X	X	
	Interoffice Mail System				
	Pay Stub				
	E-mail	X	X	X	
	Website (cannot be the only method)				
	With SPD				
	Included in New Hire Packet	X			
	Included with Open Enrollment Packet				X
	Other Method				

II. Use and Disclosure of Protected Health Information

The Company and the OHCA will use and disclose protected health information only as permitted under HIPAA. If the Company creates, receives, maintains, or transmits any electronic *protected health information* (other than enrollment / disenrollment information and summary health information, which are not subject to restrictions) on behalf of the OHCA, it will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic *protected health information*, and it will ensure that any agents (including subcontractors) to whom it provides such electronic *protected health information* agree to implement reasonable and appropriate security measures to protect the information. The Company will report any security incident of which it becomes aware.

For purposes of these policies and procedures, the term "use" means the sharing, utilization, review, examination, or analysis of individually identifiable health information by an Authorized Employee or by a Business Associate (defined in B.2. below) of the OHCA. The term "disclosure" means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to a person other than an Authorized Employee.

A. Use and Disclosure For Treatment, Payment & Health Care Operations

The OHCA is authorized to disclose protected health information to a health care provider for its provision, coordination or management of health care and related services to an individual enrolled in a group health plan that is part of the OHCA. In addition, the OHCA is authorized to disclose protected health information for its own payment purposes as well as to another covered entity for the payment purposes of that covered entity. "Payment" includes activities undertaken to obtain plan contributions or to determine or fulfill the OHCA's responsibility for provision of benefits under the OHCA, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations including coordination of benefits and adjudication (e.g., claim administration) or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

Finally, the OHCA is authorized to disclose protected health information for purposes of the OHCA's own health care operations (if any) and/or to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs.

All disclosures of protected health information for treatment, payment and health care operations as described above must comply with the "Minimum Necessary" standard (see Section IV.D. below) and be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

B. Other Permitted Uses and Disclosures of Protected Health Information

In addition to uses and disclosures relating to treatment, payment and health care operations, the OHCA is authorized to disclose protected health information to the Company for plan administration functions, to business associates if certain conditions are first satisfied, and for legal and public policy purposes, as more fully described below.

(1) *Disclosures to Plan Sponsor.* No disclosure shall be made to employees of the Company unless and until the Company amends the plan document and certifies to the OHCA, in writing, that it will only use the information in the manner permitted by HIPAA. In addition, any and all disclosures to the Company for plan administration functions must comply with the "Minimum Necessary" standard (see Section IV.D. below).

(2) *Disclosures To Business Associates.* Any and all disclosures or protected health information to a "business associate" must be made in accordance with a valid business associate agreement. A "business associate" is an entity that performs or assists in performing a plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.) or provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to protected health information. Before providing protected health information to a business associate, Authorized Employees must contact the Privacy Officer and verify that a business associate contract is in place. In addition, any and all disclosures to a business associate must be consistent with the terms of the business associate contract, must comply with the OHCA's "Minimum Necessary" standard (see Section IV.D. below) and must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

(3) *Disclosures for Legal and Public Policy Purposes.* Requests for disclosures of protected health information for the following purposes and/or in response to the following requests must be approved by the Privacy Officer, must comply with the OHCA's "Minimum Necessary" standard (see Section IV.D. below) and must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below):

- Requests needed to avert a serious threat to the health or safety of an individual or the general public.
- Requests by military command authorities.
- Requests necessary to comply with worker's compensation laws.
- Requests by organizations that handle organ donor procurement or transplantation.

- Requests relating to public health activities.
- Requests by a health oversight organization for activities authorized by law.
- Requests in the form of a court or administrative order, subpoena, discovery request, or other lawful process.
- Requests by law enforcement officials.
- Requests by a coroner, medical examiner or funeral director (as necessary to carry out their duties).
- Requests by federal officials for national security activities authorized by law.
- Requests by correctional institutions.

C. Mandatory Disclosures of Protected Health Information

Subject to the exceptions described in HIPAA, the OHCA shall disclose protected health information when requested by (i) the individual to whom the information relates or (ii) the United States Department of Health and Human Services.

(1) *Request Made By Individual.* Upon receiving a request from an individual (or an individual's representative) for disclosure of the individual's own protected health information, follow the procedure for "Right of Access to Protected Health Information" (see Section III.A. below).

(2) *Request Made by Department of Health and Human Services.* Upon receiving a request from an official of the United States Department of Health and Human Services, follow the procedures for verifying the identity of a public official set forth in the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below) and document the disclosure in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

D. Use and Disclosures Pursuant to Authorizations

The OHCA shall not use or disclose protected health information for any purpose not expressly authorized under paragraphs A, B and C immediately above unless the individual to whom the information relates has provided an authorization for such use or disclosure. If the authorization is requested by the OHCA, the Company, or an individual enrolled in a group health plan that is part of the OHCA, the authorization shall be requested on the "Authorization for Release of Protected Health Information" developed by the OHCA for this purpose, a copy of which is attached hereto as Exhibit 2.

Upon the receipt by the Contact Person of an authorization, whether the same is submitted on the OHCA's "Authorization for Release of Protected Health Information" or otherwise, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall verify the identity of the individual giving the

authorization (or individual's representative) in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below) and review the authorization to ensure it is valid. A valid authorization is one that:

- Is signed and dated by the individual or the individual's representative;
- Has not expired or been revoked;
- Contains a description of the information to be used or disclosed;
- Contains the name of the entity or person authorized to use or disclose the protected health information;
- Contains the name of the recipient of the protected health information;
- Contains a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
- Contains a statement regarding the possibility for a subsequent re-disclosure of the information.

All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the Authorization and must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

III. Individual Rights

HIPAA confers upon individuals certain rights with respect to their own protected health information that is maintained by or for the OHCA as a "designated record set." Specifically, individuals have the right to inspect and copy their protected health information; to request amendments to their protected health information; to request an accounting of disclosures of their protected health information; to request restrictions on the use and disclosure of protected health information; and to request confidential communications.

A "designated record set" is a group of records that includes the enrollment, payment, and claims adjudication record of an individual maintained by or for the OHCA and all other protected health information used, in whole or in part, by or for the OHCA to make coverage decisions about an individual.

A. Right of Access To Protected Health Information

Subject to the exceptions noted immediately below, individuals have a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set for as long as the information is maintained in the designated record set. However, and notwithstanding the foregoing, individuals do not have a right of access to inspect and obtain a copy of protected health information about the individual when:

- the information is psychotherapy notes;
- the information has been compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding;
- the information is subject to the Clinical Laboratory Improvements Amendments Act of 1988, 42 U.S.C. 263a, and access to such information is prohibited under such law;
- the information is subject to the Privacy Act, 5 U.S.C. 552a and denial of access satisfies the requirements of that law;
- the information was obtained from someone other than a health care provider under a promise of confidentiality; or
- disclosing the information is determined by a health care professional to be likely to cause harm.

All requests by an individual (or the parent of a minor or a personal representative) for access to that individual's protected health information must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request for Access to Protected Health Information," a copy of which is attached hereto as Exhibit 3 that should be used whenever possible.

Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for access to that individual's protected health information, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Ensure that the request is signed and dated.

(2) Verify the identity of the individual (or parent or personal representative) submitting the request in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below).

(3) Review the request to determine whether the requested information is held in the individual's designated record set. If it appears that the requested information is not held in the individual's designated record set, contact the Privacy Officer. No request for access may be denied without approval from the Privacy Officer.

(4) Review the request to determine whether an exception to the disclosure requirement might exist. If there is any question about whether one of the exceptions applies, contact the Privacy Officer. No request for access may be denied without approval from the Privacy Officer.

(5) Respond to the request, in writing, using the OHCA's "Response to Request for Access to Protected Health Information," a copy of which is attached hereto as Exhibit 4 (the "OHCA's Response"), within 30 days (60 days if the information is maintained

off-site). If the requested protected health information cannot be accessed within the 30 day (or 60 day) period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30 or 60 day period of the reasons for the extension and the date by which the Company will respond.

(6) If the request is not valid or is incomplete, indicate on the OHCA's Response the specific information necessary to make the request valid and/or complete and mail the Response to the individual.

(7) If the request is denied, indicate on the OHCA's Response the basis for the denial and mail the Response to the individual. No request for access may be denied without approval from the Privacy Officer.

(8) If the request is granted and the individual requested that the information be mailed to him or her, include the information with the OHCA's Response and mail it to the individual. If the individual did not request that the information be mailed to him or her, the OHCA's Response directs the individual to contact the Contact Person to arrange a mutually convenient time for the individual to review and/or copy the requested information.

All disclosures made under the forgoing procedure must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

The OHCA will not impose cost-based copying and postage charges in connection with fulfilling an individual's request for copies of his or her protected health information.

B. Right to Request Amendment to Protected Health Information

HIPAA gives individuals the right to request to have their protected health information amended. All requests by an individual (or the parent of a minor or a personal representative) for an amendment to that individual's protected health information must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request to Amend Protected Health Information," a copy of which is attached hereto as Exhibit 5 that should be used whenever possible.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for amendment of an individual's protected health information held in a designated record set, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Follow the procedures for verifying the identity of the individual (or parent or personal representative) in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below).

(2) Review the request to determine whether the protected health information at issue is held in the individual's designated record set. See the Privacy Officer if it appears that the requested information is not held in the individual's designated record set. No request for amendment may be denied without approval from the Privacy Officer.

(3) Review the request for amendment to determine whether the information would be accessible to the individual under paragraph A above. See the Privacy Officer if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Officer.

(4) Review the request for amendment to determine whether the amendment is appropriate - that is, determine whether the information in the designated record set is accurate and complete without the amendment.

(5) Respond to the request, in writing, using the OHCA's "Response to Request to Amend Protected Health Information," a copy of which is attached hereto as Exhibit 6 (the "OHCA's Response"), within 60 days. If the determination cannot be made within the 60 day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60 day period of the reasons for the extension and the date by which the Company will respond.

(6) When a request for amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.

(7) When a request for amendment is denied, the OHCA's Response shall be approved by the Privacy Officer. The OHCA's response must set forth (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial. If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and the Company's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

C. Right to Request Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own protected health information made after April 14, 2004. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations; however, if the disclosure involves a disclosure of an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized healthcare clinicians and staff, this must be accounted for and records maintained for three (3) years;

- to individuals about their own protected health information;

- incident to an otherwise permitted use or disclosure;

- pursuant to an authorization;

- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;

- as part of a limited data set; or

- for other national security or law enforcement purposes.

All requests by an individual (or the parent of a minor or a personal representative) for an accounting of disclosures of that individual's protected health information must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request for Accounting of Disclosures of Protected Health Information," a copy of which is attached hereto as Exhibit 7, that should be used whenever possible.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosure of an individual's protected health information, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Follow the procedures for verifying the identity of the individual (or parent or personal representative) in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below).

(2) Respond to the request, in writing, using the OHCA's "Response to Request for Accounting of Disclosures of Protected Health Information," a copy of which is attached hereto as Exhibit 8, within 60 days by enclosing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting. If the accounting cannot be provided within the 60 day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60 day period of the reasons for the extension and the date by which the Company will respond.

(3) The accounting must include disclosures (but not uses) of the requesting individual's protected health information made by the OHCA and any of its business associates during the period requested by the individual up to six years prior to the request. (Note: the OHCA is not required to account for any disclosures made prior to the compliance date.)

(4) If any business associate of the OHCA or a group health plan that is part of the OHCA has the authority to disclose the individual's protected health information, the Contact Person shall request an accounting of disclosure from such business associate.

(5) The accounting must include the following information for each reportable disclosure of the individual's protected health information:

- the date of disclosure;
- the name (and if known, the address) of the entity or person to whom the information was disclosed;
- a brief description of the protected health information disclosed; and
- a brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)

Accountings must be documented in accordance with the OHCA's "Documentation" policy and procedures (see Section IV.A. below).

The OHCA will not impose cost-based charges in connection with the production, copying and mailing of an individual's request for an accounting of disclosures of his or her protected health information.

D. Right to Request Alternative Communications

Individuals may request to receive communications regarding their protected health information by alternative means or at alternative locations. For example, an individual may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the Company, the requests are reasonable. However, the Company shall accommodate such a request if the individual clearly provides information that the disclosure of all or part of that information could endanger the individual. The Privacy Officer has responsibility for administering requests for confidential communications.

All requests by an individual (or the parent of a minor or a personal representative) for alternative communications must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request for Confidential Communications," a copy of which is attached hereto as Exhibit 9, that should be used whenever possible.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of protected health information by alternative means or at alternative locations, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Follow the procedures for verifying the identity of the individual (or parent or personal representative) in accordance with the OHCA's "Verification of Identity" policy and procedure (see Section IV.B. below).

(2) Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual. Requests for confidential and/or alternative communications must be honored by the OHCA if the individual states that disclosure could endanger the individual.

(3) Respond to the request, in writing, using the OHCA's "Response to Request for Confidential Communications," a copy of which is attached hereto as Exhibit 10 and indicate on the OHCA's Response whether the request will be accommodated.

(4) If a request will not be accommodated, the OHCA's Response shall explain why the request cannot be accommodated.

(5) All Requests for Confidential Communications and responses thereto shall be reviewed by the Privacy Officer.

Requests and their dispositions must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

E. Right to Request Restrictions

An individual may request restrictions on the use and disclosure of the individual's protected health information. It is the Company's policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable.

All requests by an individual (or the parent of a minor or a personal representative) for restrictions on the use and disclosure of the individual's protected health information must be in writing and signed by the individual (or the parent of a minor or a personal representative). The OHCA has developed a "Request for Restrictions to Protected Health Information," a copy of which is attached hereto as Exhibit 11, that should be used whenever possible.

Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to restrict access to an individual's protected health information, the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) shall:

(1) Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in the "Verification of Identity" policy and procedure (see Section IV.B. below).

(2) Respond to the request, in writing, using the OHCA's "Response to Request for Restrictions to Protected Health Information," a copy of which is attached hereto as Exhibit 12 and indicate on the OHCA's Response whether the request will be accommodated.

(3) If a request will not be accommodated, the OHCA's Response shall explain why the request cannot be accommodated. Note, however, if the request relates to restricting the disclosure of PHI to another health plan and it pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket in full and where the purpose of the disclosure is for carrying out payment or health care operations, the OHCA must agree to the request for restrictions to such PHI.

(4) All Requests for Restrictions to Protected Health Information and responses thereto shall be reviewed by the Privacy Officer.

Requests and their dispositions must be documented in accordance with the OHCA's "Documentation" policy and procedure (see Section IV.A. below).

IV. Administrative Provisions and Safeguards

A. Documentation

The OHCA shall maintain copies of the OHCA's Notice of Privacy Practices and Individual Authorizations for a period of at least six years from the date the documents were created or were last in effect, whichever is later. In addition, when a disclosure of protected health information is made, the Authorized Employees making such disclosure shall indicate on the OHCA's "Disclosure Report" form, a copy of which is attached hereto as Exhibit 13: (i) the date of the disclosure; (ii) the name of the entity or person who received the protected health information and, if known, the address of such entity or person; (iii) a brief description of the information disclosed; (iv) a brief statement of the purpose of the disclosure; and (v) any other documentation required under the Use and Disclosure policies and Procedures (as applicable).

B. Verification of Identity

The OHCA must take steps to verify the identity of individuals who request access to protected health information. The OHCA must also verify the authority of any person to have access to protected health information if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the protected health information of his or her minor child, a personal representative, or a public official seeking access.

(1) *Request Made by Individual.* When an individual requests access to his or her own protected health information, unless the Authorized Employee knows from personal experience that the individual is who or she purports to be, the following steps should be followed:

(a) Request a form of identification from the individual. The OHCA will accept a valid driver's license, passport or other photo identification issued by a government agency.

(b) Verify that the identification matches the identity of the individual requesting access to the protected health information. If there is any doubt as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the protected health information, the Privacy Officer should be contacted.

(c) Make a copy of the identification provided by the individual and file it with the individual's designated record set.

(d) If the individual requests protected health information over the telephone, instruct the individual that it is the OHCA's policy that all requests for access to protected health information must be submitted in writing to the Contact Person.

(2) *Request Made by Parent of a Minor Child.* When a parent requests access to the protected health information of the parent's minor child, unless the Authorized Employee knows from personal experience that the individual is the parent of the minor child to whom the information relates, request verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. Make a copy of the documentation provided and file it in the individual's designated record set.

(3) *Request Made by Personal Representative*. When a personal representative requests access to an individual's protected health information, request a copy of appropriate documentation such as a valid power of attorney. If there are any questions about the validity of this document, seek review by the Privacy Officer. Make a copy of the documentation provided and file it in the individual's designated record set.

(4) *Request Made by Public Official.* If a public official requests access to protected health information, and if the request is for one of the purposes set forth above in Section II.B.3. (relating to disclosures for legal and public policy purposes) or Section II.C.2 (relating to disclosures to the Department of Health and Human Services), the following steps should be followed to verify the official's identity and authority:

(a) If the request is made in person, request presentation of an agency identification badge, other official credentials or other proof of government status. Make a copy of the identification provided and file it in the individual's designated record set.

(b) If the request is in writing, verify that the request is on the appropriate government letterhead;

(c) If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or

other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(d) Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Privacy Officer.

(e) Obtain approval for the disclosure from the Privacy Officer.

(5) *Request Made by Spouse, Family Member or Friend.* The OHCA and Company will not disclose protected health information to family and friends of an individual except as required or permitted by HIPAA. The OHCA will not disclose an individual's protected health information to any person, including a spouse, family member or friend, unless the individual to whom the information relates is present (and does not object) or the OHCA or group health plan that is part of the OHCA has received a valid authorization. If the individual to whom the information relates is not present or is not capable of consenting to the disclosure because of the individual's incapacity or emergency circumstances, the OHCA may disclose protected health information to the spouse, family member or friend of an individual, if, in the exercise of professional judgment, the OHCA determines it is in the best interests of the individual to make the disclosure.

If the Contact Person (or Authorized Employee acting under the direction and supervision of the Contact Person) receives a request for disclosure of an individual's protected health information from a spouse, family member, or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child, or (2) the personal representative of the individual, then follow the applicable "Verification of Identity" policy and procedure (see Section IV.B. above). Once the identity of a parent or personal representative is verified, follow the OHCA's "Right of Access to Protected Health Information" policy and procedure (see Section III.A. above). All other requests from spouses, family members, and friends must be authorized by the individual whose protected health information is involved in accordance with the OHCA's policy and procedures for "Use and Disclosures Pursuant to Authorizations" (see Section II.D. above).

C. Record Storage and Access

The Company is required to establish, on behalf of the OHCA, appropriate technical and physical safeguards to prevent protected health information from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

(1) *Physical Safeguards*. All designated records sets shall be maintained separately and secured separately from all employee records. Designated record sets shall not be commingled with employment records of any kind. To ensure that paper files will be safeguarded from unauthorized public view, Authorized Employees shall store designated record sets in locked filing cabinets or in a locked file room. Only Authorized Employees with authorization from the Contact Person or Privacy Officer shall have access to the locked file cabinets and/or locked area. While unattended, the file system will not be left open.

(2) *Technical Safeguards*. Any and all protected health information stored on computers will be password protected. Only Authorized Employees with authorization from the Contact Person or Privacy Officer will have access to any and all of such computer files. Any protected health information copied onto removable media, including backup media, will be protected in the same manner as paper files, as outlined above. Any material that contains protected health information will, while in use, be protected from deliberate or casual oversight by passers-by. Computer screens displaying protected health information will be turned away from public areas so as not to be visible to passers-by in public areas.

(3) *Disposal*. Any and all handwritten notes such as phone messages and reminder slips containing protected health information must be shredded as soon as they are no longer needed. Dictation tapes containing protected health information must be erased after the material is transcribed. All unwanted or duplicate papers containing protected health information must be shredded immediately after it is determined that they are no longer needed. Any electronic media containing protected health information is wiped when the data is no longer required. Hard drives must be reformatted when an office computer is sold, or when Authorized Employees no longer use it to access protected health information. If they contain protected health information, CDs must be destroyed when the data is no longer required.

D. Minimum Necessary Standard

HIPAA requires that when protected health information is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure. “Minimum necessary” means (1) for electronic information, reviewing, forwarding, or printing out only those fields and records relevant to the user’s need for information, and (2) for non-electronic information, the selective copying of relevant parts of protected health information.

The "minimum necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to the United States Department of Health and Human Services;

- uses or disclosures required by law; and

- uses or disclosures required to comply with HIPAA.

With respect to requests for information from business associates, the OHCA shall limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. In addition and whenever possible, the OHCA shall use de-identified information if the purpose of the disclosure could be reasonably accomplished with information that is not identifiable. De-identified information is information with all of the following elements removed:

- Names;

- All geographic subdivisions smaller than a state, except a three-digit zip code may be used under certain circumstances;

- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

- Telephone numbers;

- Fax numbers;

- Electronic mail addresses;

- Social security numbers;

- Medical record numbers;

- Health plan beneficiary numbers;

- Account numbers;

- Certificate/license numbers;

- Vehicle identifiers and serial numbers, including license plate numbers;

- Device identifiers and serial numbers;

- Web Universal Resource Locators (URLs);

- Internet Protocol (IP) address numbers;

- Biometric identifiers, including finger and voice prints;

- Full face photographic images and any comparable images; and

- Any other unique identifying number, characteristic, or code.

The OHCA shall not disclose an individual's entire designated record set unless the request for disclosure includes an explanation of why the purpose of the disclosure could not reasonably be accomplished without the entire designated record set. Similarly, the OHCA shall not disclose an individual's entire designated record set in response to a request for more limited data. In the day-to-day operation of the OHCA and the Company, physical access to protected health information, whether in paper or electronic media, shall be limited to Authorized Employees.

E. Mitigation of Inadvertent Disclosures

HIPAA requires that the OHCA mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's protected health information in violation of this Privacy Policy. As a result, if an Authorized Employee becomes aware of a disclosure of protected health information, either by an Authorized Employee or a business associate of the OHCA or a group health plan that is part of the OHCA, that is not in compliance with the policies and procedures of the OHCA, such Authorized Employee shall immediately contact the Privacy Officer so that the appropriate steps to mitigate any potential harm to the individual can be taken.

F. Employee Training

HIPAA requires that protected health information is protected against unauthorized use or disclosure. To that end, the Company, in its capacity as the plan sponsor, is responsible for training all members of its workforce with respect to its privacy policies and procedures. Specifically, the OHCA must:

- provide training to each member of the workforce who is authorized to have access to protected health information prior to the compliance date;

- provide training to all new employees who will be authorized to have access to protected health information within a reasonable time after they join the workforce;

- provide training to all new employees who may be authorized to have access to protected health information upon the occurrence of an unanticipated or unusual event. Access under these circumstances shall be limited in time and scope. Basic training may be provided within a reasonable time after such employee joins the workforce. Such training shall be followed by any additional training that may be necessary at the time of the unanticipated or unusual event;

- retrain each member of the workforce who is authorized to have access to protected health information when and to the extent that material changes in policies and procedures are made; and

- document the training on the OHCA's "Employee Training Log," a copy of which is attached hereto as Exhibit 14.

(1) *Existing Employee Training*. All existing employees of the Company with access to protected health information will receive a privacy orientation. The employee's supervisor or other trainer will explain the HIPAA privacy regulations as they relate to the employee's job, their importance, and how the Company has responded to these regulations. Each employee with access to protected health information will receive a copy of this Privacy Policy and will be asked to sign a statement indicating that they have read, understand and agree to abide by all policies and procedures set forth in the Privacy Policy, and further understand that the penalties for not following the Privacy Policy could include severe disciplinary action, up to and including termination. The written statement which is entitled "Employee Acknowledgment" and is attached hereto as Exhibit 15, shall be retained by the OHCA.

(2) *New Employee Training*. All new employees of the Company with access to protected health information will receive a privacy orientation. The employee's supervisor or other trainer will explain the HIPAA privacy regulations as they relate to the employee's job, their importance, and how the Company has responded to these regulations. Each new employee with access to protected health information will receive a copy of this Privacy Policy and will be asked to sign the "Employee Acknowledgment" form, which is attached hereto as Exhibit 15, indicating that they have read, understand and agree to abide by all policies and procedures set forth in the Privacy Policy, and further understand that the penalties for not following the Privacy Policy could include severe disciplinary action, up to and including termination.

The Privacy Officer is responsible for ensuring that appropriate education and procedures are in place and enforced to assure senior management that new employees are trained properly regarding privacy and confidentiality and in accordance with our policies and the relevant statutes.

G. Sanctions for Violations of Policies and Procedures

The Company will apply appropriate sanctions against any employee who violates the policies and procedures set forth herein. Authorized Employees are provided training (and retraining as necessary) to ensure they understand all of the policies and procedures that apply to protected health information. Appropriate sanctions for violations of the OHCA's policies and procedures will be determined with reference to the nature of the violation, the severity of the violation and whether the violation was intentional or unintentional. Sanctions may include verbal warnings, written warnings, imposition of probationary periods or termination.

H. Complaints

HIPAA requires that a group health plan create a process for individuals to submit complaints regarding the OHCA's policies and procedures and create a system for handling such complaints. The OHCA's Notice of Privacy Practice and related forms state that if the individual is dissatisfied with the OHCA in regard to the individual's protected health information request, the individual may file a complaint with the Contact Person (who will deliver the complaint to the Privacy Officer) or the Department of Health and Human Services. If an individual exercised his or

her right to file a written complaint with the Contact Person, the Privacy Officer, upon receipt of the complaint, shall log the complaint in a separate file maintained exclusively for this purpose. In addition, in response to any such complaint, the Privacy Officer shall:

(1) investigate the complaint and document his or her findings;

(2) document the decision regarding whether a violation actually occurred, and any resolution regarding the alleged violation, regardless of determination;

(3) if a procedure change in policy or procedure is warranted, the Privacy Officer shall implement the necessary changes or modifications, amend the Policy to be consistent with those changes or modifications, and communicate the changes to all Authorized Employees; and

(4) correspond, in writing, with the individual filing the complaint and indicate what, if any, action the OHCA will take with respect to the complaint (such action may include an apology and/or a description of the change in policies or procedures to prevent similar complaints in the future).

If the Privacy Officer is unable to resolve the complaint, the individual should be advised to file a complaint with the Office for Civil Rights of the United States Department of Health and Human Services. The address of the Department varies depending on the location of the individual who wishes to file the complaint. To file a complaint with the OHCA, contact the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with the OHCA.

V. Electronic Security

A. Risk Analysis

The OHCA has developed a "Risk Analysis Worksheet," a copy of which is attached hereto as Exhibit 16. The Worksheet documents the OHCA's electronic security analysis.

The OHCA has no employees. All of the OHCA's functions, including creation and maintenance of its records, are carried out by Authorized Employees of the Company, by business associates of the OHCA, by business associates of a group health plan that is part of the OHCA, or by the insurer. The OHCA does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the OHCA, or any of the facilities in which such equipment and media are located. Such equipment, media and facilities are owned or controlled by the Company, its business associates, and the insurer. Accordingly, the Company, its business associates, and the insurer create and maintain all of the electronic PHI relating to the OHCA, own or control all of the equipment, media and facilities used to create, maintain, receive, or transmit electronic PHI relating to the OHCA, and control their employees, agents, and subcontractors who have access to electronic PHI relating to the OHCA. The OHCA has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the OHCA. That ability lies solely with the Company, its business associates, and the insurer.

Because the OHCA has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Company and its business associates affecting the security of electronic PHI relating to the OHCA, and the Company and its business associates have undertaken certain obligations relating to the security of electronic PHI that they handle in relation to the performance of administration functions for the OHCA, the OHCA's policies and procedures, including this Policy, do not address the following standards (including the implementation specifications associated with them) established under HIPAA and are set out in Subpart C of 45 C.F.R. Part 164:

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

B. Plan Document

The plan document shall include provisions requiring the Company to:

(1) implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the Company creates, receives, maintains, or transmits on behalf of the group health plans that are part of the OHCA (the OHCA's electronic PHI);

(2) ensure that reasonable and appropriate security measures support the plan document provisions providing for adequate separation between the OHCA and the Company;

(3) ensure that any agents or subcontractors to whom the Company provides electronic PHI agree to implement reasonable and appropriate security measures to protect the OHCA's electronic PHI; and

(4) report to the Security Officer any security incident of which the Company becomes aware.

C. Disclosures of Electronic PHI to Business Associates

In the future, the OHCA may permit one or more business associates to create, receive, maintain, or transmit electronic PHI on its behalf only if the OHCA or the group health plan that is part of the OHCA first obtains satisfactory assurances from the business associate that it will appropriately safeguard the information, pursuant to 45 C.F.R. Parts 160 and 164. Such satisfactory assurances shall be documented through a written contract providing that the business associate will:

(1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the OHCA or the group health plan that is part of the OHCA;

(2) ensure that any agents or subcontractors to whom the business associate provides electronic PHI enter into a contractual arrangement with the business associate in which they agree to implement reasonable and appropriate security measures to protect the electronic PHI;

(3) immediately report to the OHCA or the group health plan that is part of the OHCA any security incident of which the business associate becomes aware; and

(4) authorize termination of the contract by the OHCA or the group health plan that is part of the OHCA if the OHCA or the group health plan that is part of the OHCA determines that the business associate has violated a material term of the contract.

D. Documentation

The OHCA's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of the OHCA's electronic PHI, and any changes to policies or procedures will be documented promptly.

Except to the extent that they are carried out by the Company, business associates, or the insurer, the OHCA shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented (including amendment of the plan document in accordance with this policy, for example).

Policies, procedures, and other documentation controlled by the OHCA may be maintained in either written or electronic form. The OHCA will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The OHCA will make its policies, procedures, and other documentation available to the Security Officer and the Company, as well as business associates or other persons responsible for implementing the procedures to which the documentation pertains.

VI. Breach Notifications

The OHCA will comply with the requirements of the Health Information Technology for Economic and Clinical Health ("HITECH") Act and its implementing regulations to provide notification to affected individuals, HHS and the media (when required) if the OHCA or one of its business associates discovers a Breach of Unsecured PHI.

A. Definitions of Breach / Unsecured PHI

(1) *"Breach"* means the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such Protected Health Information. The following three types of unauthorized acquisition, access, use, or disclosure are excluded from the definition of a Breach:

(a) Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the OHCA if such acquisition, access, or use was made in good faith and within the course and scope of employment or other professional relationship of such employee or individual with the OHCA, and the information is not further acquired, accessed, used, or disclosed by any person in a manner not permitted by the Privacy and/or Security Rules;

(b) Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by the OHCA to another similarly situated individual at the same facility so long as the information received is not further used or disclosed in a manner not permitted by the Privacy and/or Security Rules; and

(c) Any disclosure to an unauthorized person where the PHI that was disclosed would not reasonably have been retained by such person.

(2) *"Unsecured Protected Health Information"* means Protected Health Information that is not secured through the use of a technology or methodology specified by the Secretary of Health and Human Services ("HHS") through guidance issued by the Secretary.

B. Breach Determination and Risk Analysis

(1) *Breaches by a Business Associate.* Under the HITECH Act, a business associate must timely notify the OHCA or the group health plan that is part of the OHCA if it discovers or should have discovered (using reasonable diligence) a Breach of Unsecured PHI. If a business associate informs the OHCA or the group health plan that is part of the OHCA that it has discovered a Breach of Unsecured PHI, the OHCA or the group health plan that is part of the OHCA will consult the business associate agreement which is in place with the business associate in question in order to determine if the business associate agreed to make any of the notifications on behalf of the OHCA or the group health plan that is part of the OHCA to individuals, HHS or, if applicable,

the media. To the extent that the business associate did *not* agree to make the necessary notifications to affected individuals, the OHCA or the group health plan that is part of the OHCA will make such notification(s) in accordance with VI.C.(1), (2) and/or (3) below.

(2) *Breaches by the OHCA.* The OHCA will perform a risk assessment to determine if a Breach of Unsecured PHI has occurred. The acquisition, access, use, or disclosure of PHI in an impermissible manner is presumed to be a Breach unless the OHCA can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment as set forth in 45 C.F.R. 164.402(2). The "Breach Determination – Risk Assessment: (Exhibit 17) shall be used to perform this analysis. If it is determined that there is a Breach of Unsecured PHI, certain notifications need to be made to individuals, HHS, and potentially, the media. These notifications shall be made in accordance with VI.C.(1), (2) and/or (3) below.

C. Breach Notifications

If, after performing a risk assessment, it is determined that a Breach of Unsecured PHI has occurred, the OHCA will notify the following parties, as applicable:

(1) *Individuals.* All individuals whose Unsecured PHI has been or is reasonably believed by the OHCA to have been accessed, acquired, used, or disclosed as a result of a Breach of Unsecured PHI shall be notified of the Breach without unreasonable delay and in no case later than 60 calendar days after the Breach is discovered (or should have been discovered through exercising reasonable diligence).

The notification shall include, to the extent possible, the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of Unsecured PHI involved in the Breach (such as whether the full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
- A brief description of what the OHCA is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, e-mail address, website, or postal address.

The notification shall be written in plain, easy-to-understand language. The written notification shall be sent by 1st class mail to the individual at his/her last known address. If the individual agrees to electronic notice and has not withdrawn such agreement, the notification may be sent via electronic mail. One or more mailings may be made as additional information becomes available.

If the OHCA knows that the individual is deceased and has the address of the next of kin or personal representative, written notification by 1st class mail to either the next of kin or personal representative of the individual.

If there is insufficient or out-of-date contact information which would prevent the OHCA from making the proper notification, a substitute form of notice which is reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative. If there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone or other means.

(2) *Media.* The media need only be notified if the Breach of Unsecured PHI involved more than 500 residents of a State or jurisdiction. If more than 500 residents of a State or jurisdiction are involved, the OHCA will notify prominent media outlets serving that State or jurisdiction of the Breach. This notification will be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.

(3) *HHS.* If there is a Breach of Unsecured PHI the Secretary of HHS will be notified. The timing of this notification and the type of notification depend on whether or not the Breach involved 500 or more individuals, as follows:

(a) *Breaches Involving 500 or More Individuals.* If a Breach of Unsecured PHI involves 500 or more individuals, the OHCA will notify the Secretary of HHS at the same time the individual notice is given. The manner for notifying the Secretary is set forth on the HHS website.

(b) *Breaches Involving Less than 500 Individuals.* If a Breach of Unsecured PHI involves less than 500 individuals, the OHCA will maintain a log or other documentation of the Breaches and notify the Secretary of HHS of these Breaches within 60 days after the end of the calendar year in which the Breaches were discovered. The OHCA will consult the HHS website for instructions for submitting the notification. A log for keeping track of Breaches is found behind Exhibit 18 to these Policies and Procedures.

D. Law Enforcement Delay

The OHCA must temporarily delay any notification if it is instructed by a law enforcement official to delay notification. The law enforcement official must provide a written statement justifying the delay and indicating a time period for the delay.

For example, a delay may be necessary if the required notification would impede a criminal investigation. If only an oral statement is provided by the law enforcement official, the OHCA must document the statement and the identity of the official. The maximum period of delay where only an oral statement has been given is 30 days.

See *Notices of Privacy Practices*
tab of this Handbook
for Privacy Notices
(the full version and
the reminder notice)

Barton County Community College Organized Health Care Arrangement
Authorization for Release of Protected Health Information

Uses and disclosures of your protected health information not otherwise described in the Notice of Privacy Practices or the laws that apply to the Barton County Community College Organized Health Care Arrangement (the "OHCA") will be made only with your written permission. If you want the OHCA to disclose your protected health information in a manner or to a person not otherwise described in the Notice of Privacy Practices or the laws that apply to the OHCA, please provide the information requested below, sign this Request and submit it to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, Monday through Friday during the hours of 8 a.m. and 5 p.m. In the alternative, you may submit this Authorization by depositing it in the United States mail, postage prepaid, and addressed to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530.

Individual Information. Please provide the following information:
Name: _____
Date of Birth: ____/____/____
Social Security Number:_____
Address: _____
Telephone Number: _____

Identification of Information to Which This Authorization Applies. I hereby request the OHCA to release and disclose the protected health information specified below (please check one or more):

☐ Full record. ☐ Full record for the period ____/____/____ to ____/____/____.
☐ Enrollment information. ☐ Premium / contribution payment information.
☐ Claims and billing information relating to the following service or claim (specify date of service and/or medical condition): _____
_____

☐ Other (please specify): _____
_____

Identification of Persons/Organization to Which This Authorization Applies. I hereby request that the following persons or organizations be allowed to use and/or receive the protected health information specified above:

_____
_____

Expiration Date of Authorization. This Authorization shall remain in effect until (specify a date or an event relating to you personally or to the purpose of this Authorization):

_____
_____

Your Rights. By signing and submitting this Authorization, you acknowledge the following statements about your rights: (1) This Authorization is voluntary and you are not required to sign it; (2) You are not required to sign this Authorization to receive health care benefits under the OHCA; (3) You may revoke this Authorization at any time prior to its expiration date by notifying the OHCA in writing, however, the revocation will have no effect on any actions the OHCA may have taken prior to receipt of your revocation; (4) You have the right to inspect and copy the protected health information covered by this Authorization; (5) The information that is to be used or disclosed pursuant to this Authorization may be disclosed by the person(s) or organization(s) authorized by you to receive the information; and (6) You may revoke this Authorization at any time. Your revocation of this Authorization must be in writing and must be signed by you.

_____ _____

Signature Date

_____

Print Name

Please Note: If this form is signed and submitted by a person other than the individual identified above, the OHCA will require verification of the authority of the person signing on behalf of the individual before this request will be considered complete.

Barton County Community College Organized Health Care Arrangement
Request for Access to Protected Health Information

You have the right to inspect and copy certain protected health information that may be used to make decisions about your benefits under the Barton County Community College Organized Health Care Arrangement (the "OHCA"). If you want to inspect and/or copy your protected health information held by the OHCA, please provide the information requested below, sign this Request and submit it in person to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, Monday through Friday during the hours of 8 a.m. and 5 p.m. In the alternative, you may submit this Request by depositing it in the United States mail, postage prepaid, and addressed to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530.

Individual Information. Please provide the following information:
Name: _____
Date of Birth: ____/____/____
Social Security Number:_____
Address: _____
Telephone Number: _____

Identification of Requested Information. I hereby request from the OHCA access to the protected health information specified below (please check one or more):

☐ Full record. ☐ Full record for the period ____/____/____ to ____/____/____.
☐ Enrollment information. ☐ Premium / contribution payment information.
☐ Claims and billing information relating to the following service or claim (specify date of service and/or medical condition): _____
_____

☐ Other (please specify):_____
_____

Desired Method of Receipt of Requested Information. I understand that I may access my protected health information through the following methods (please check the desired method):

☐ I prefer to inspect and/or copy the requested information in person.

☐ I prefer to have the requested information copied and mailed to me at the address above.

The OHCA's Obligation. You will be notified by the OHCA, in writing, of the OHCA's decision regarding this Request. Generally, the OHCA is required by law to act on this Request no later than 30 days after the receipt of this Request. However, if the requested information is not maintained by, or accessible to, the OHCA, the OHCA is required to act on this Request no later than 60 days after receipt. In very limited circumstances, the OHCA may deny your request to inspect and copy protected health information. If you are denied access to your protected health information, you will be notified in writing of the reasons why access was denied and your appeal rights will be fully explained to you.

Signature _____ Date _____

Print Name _____

Please Note: If this form is signed and submitted by a person other than the individual named above, the OHCA will require verification of the authority of the person signing on behalf of the individual for whom access is being requested.

Office Use Only		
Reviewed by:	Initials:	Date Reviewed:
Decision: ____ Approved or ____ Denied.		Decision Notification Sent:
Response Approved by:		Date:

Barton County Community College Organized Health Care Arrangement
Response to Request for Access to Protected Health Information

To:_____

The OHCA has received and reviewed your Request for Access to Protected Health Information. You are hereby notified that (check one):

☐ **The OHCA Requires Additional Time to Respond to Your Request.** The reason for the delay is:_____
_____
_____

The requested information will be provided, or made available, to you no later than _____ (may not exceed 30 days beyond the original 30/60 day response period).

☐ **The OHCA is Granting Your Request.** If you requested that the information be mailed to you, the information is enclosed with this letter. If you requested to inspect and/or copy the requested information in person, please call the Benefit Specialist at (620) 792-9235 during regular business hours to arrange for a mutually convenient time to view and/or copy the requested information.

☐ **The OHCA is Denying Your Request.** The basis for this denial is as follows (check one or more as appropriate):

☐ The requested information is excepted from the right of access by regulation section 164.524 paragraph (a)(1) or (a)(2) of the Health Insurance Portability and Accountability Act of 1996 because the information (1) is psychotherapy notes; (2) has been compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding; (3) is subject to the Clinical Laboratory Improvements Amendments Act of 1988, 42 U.S.C. 263a, and access to such information is prohibited under such law; or (4) is subject to the Privacy Act, 5 U.S.C. 522a and denial of access satisfies the requirements of that law. **Please Note**: If you are denied access to your protected health information for any of the four reasons listed immediately above, you are not entitled to appeal the denial.

☐ A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of you or another person.

☐ The requested information makes reference to another person and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.

☐ The request was made by a personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that allowing access to such personal representative is reasonably likely to cause substantial harm to the individual to whom the information relates or to another person.

If you are denied access to your protected health information based upon the professional judgment of a licensed health care professional, you have the right to have the denial reviewed by a licensed health care professional who is designated by the OHCA to act as a reviewing official and who did not participate in the original decision to deny access. You must submit a written statement to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, disagreeing with this denial and explaining your reasons for disagreement. You will receive a written response of the reviewing official.

Complaints. If you are dissatisfied with the OHCA's decision, you may file a complaint with the OHCA and with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the OHCA, contact the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with us.

Barton County Community College Organized Health Care Arrangement
Request to Amend Protected Health Information

If you feel that protected health information the Barton County Community College Organized Health Care Arrangement (the "OHCA") has about you is incorrect or incomplete, you have the right to ask the OHCA to amend the information. You have the right to request an amendment for as long as the information is kept by or for the OHCA. To request an amendment, please provide the information requested below, sign this Request and submit it in person to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, Monday through Friday during the hours of 8 a.m. and 5 p.m. In the alternative, you may submit this Request by depositing it in the United States mail, postage prepaid, and addressed to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530.

Individual Information. Please provide the following information:
Name: _____
Date of Birth: ____/____/____
Social Security Number:_____
Address: _____
Telephone Number: _____

Identification of Information For Which Amendment is Requested. I am requesting that the OHCA amend my protected health information in the manner described below. I understand the OHCA must determine if the requested amendment is permitted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations issued thereunder. I further understand the OHCA may not be able to honor this request. The following is a description of the specific information I wish to amend and the reasons I wish to amend it (please be as specific as possible):_____
_____
_____
_____
_____
_____
_____
_____

The OHCA's Obligation. The OHCA is required by law to act on this Request no later than 60 days after receipt. You will be notified, in writing, within 60 days of the date of this Request, whether the requested amendment will be granted. If your requested amendment is allowed, it will be maintained as part of your record. The OHCA may deny your request if you ask the OHCA to amend information that:

- is not part of the information kept by or for the OHCA;
- was not created by the OHCA, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the information which you would be permitted to inspect and copy; or
- is accurate and complete.

Signature _____ Date _____

Print Name _____

Please Note: If this form is signed and submitted by a person other than the Participant identified above, the OHCA will require verification of the authority of the person signing on behalf of the Participant before this request will be considered complete.

Barton County Community College Organized Health Care Arrangement
Response to Request to Amend Protected Health Information

To:_____

The OHCA received and reviewed your Request to Amend Protected Health Information. You are hereby notified that (check one):

☐ **The OHCA Requires Additional Time to Respond to Your Request.** The reason for the delay is:

_____

_____

_____

The requested information will be provided or made available to you no later than _____ (may not exceed 30 days beyond the original 60 day response period).

☐ **Your Request is Incomplete.** Your request is being returned to you because it is incomplete. Your request is incomplete in the following way(s):_____

_____

A new Request to Amend Protected Health Information is enclosed. Please resubmit your request.

☐ **The OHCA is Accepting Your Request.** Your requested amendment will be maintained as part of your record.

☐ **The OHCA is Denying Your Request.** The basis for the denial is as follows (check one or more as appropriate):

☐ The protected health information for which you requested an amendment to is not part of the information kept by or for the OHCA.

☐ The OHCA did not create the protected health information for which you requested an amendment and the OHCA reasonably believes the person or entity that created the information is still available to make the amendment.

☐ The protected health information for which you requested an amendment is not part of the information which you would be permitted to inspect and copy.

☐ The protected health information for which you requested is accurate and complete.

Your Rights. If the OHCA has denied your request, you have the right to submit a written statement disagreeing with the denial. You must submit your written statement to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, and explain your reasons for disagreement. If you chose not to submit a written statement, you may request that the OHCA provide a copy of your Request to Amend Protected Health Information with any future disclosures of the protected health information that is the subject of the requested amendment. You must request that the OHCA provide a copy of your Request to Amend Protected Health Information with any future disclosures of the protected health information that is the subject of the requested amendment in writing and submit the same to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530.

Complaints. If you are dissatisfied with the OHCA's decision, you may file a complaint with the OHCA and with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the OHCA, contact the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with us.

Barton County Community College Organized Health Care Arrangement
Request for Accounting of Disclosures of Protected Health Information

---

You have the right to request an accounting of certain disclosures of your protected health information made by the Barton County Community College Organized Health Care Arrangement (the "OHCA"). To request an accounting of disclosures, please provide the information requested below, sign this Request and submit it in person to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, Monday through Friday during the hours of 8 a.m. and 5 p.m. In the alternative, you may submit this Request by depositing it in the United States mail, postage prepaid, and addressed to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530.

Individual Information. Please provide the following information:
Name: _____
Date of Birth: ____/____/____
Social Security Number: _____
Address: _____
Telephone Number: _____

Request for Accounting. I am requesting that the OHCA provide to me an accounting of all non-routine uses and disclosures of my protected health information for the period identified below. I understand that the accounting will **NOT** include the following routine uses and disclosures: (1) those provided for purposes of treatment, payment, or health care operations, unless they involve a disclosure of an electronic record of health-related information that is created, gathered, managed and consulted by authorized healthcare clinicians and staff; (2) those provided to me; (3) those made pursuant to my written authorization; (4) those made to friends or family in my presence or because of an emergency; (5) those provided for national security purposes; (6) those provided to correctional institutions or law enforcement officers; and (7) those incidental to an otherwise permissible disclosure.

Reporting Period. This Request is for all non-routine uses and disclosures of my protected health information beginning _____ and ending _____ (the total period may not exceed 6 years (or 3 years in the case of the disclosure of electronic health records)).

Fees. I understand I will not be charged for the first accounting requested by me in any 12-month period. However, if I submit more than one Request for Accounting of Disclosures of Protected Health Information during any 12-month period, I acknowledge that the OHCA may charge me a cost-based fee for each such subsequent request. If you have previously submitted a Request for Accounting of Disclosures of Protected Health Information during the preceding 12-month period, please contact the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, (620) 792-9235, to receive an estimate of the cost of this Request.

Desired Method of Receipt of Requested Information. I understand that I may receive an accounting of the non-routine disclosures of my protected health information through the following methods (please check the desired method):

☐ I prefer to receive an accounting of the non-routine disclosures of my protected health information in person.

☐ I prefer to receive an accounting of the non-routine disclosures of my protected health information mailed to me at the address above.

The OHCA's Obligation. You will be notified by the OHCA, in writing, of the OHCA's decision regarding this Request. Generally, the OHCA is required by law to act on this Request no later than 60 days after receipt of this Request. However, if the OHCA is unable to meet this 60 day requirement, the OHCA may extend the period for an additional 30 days.

_____ _____

Signature Date

_____

Print Name

Please Note: If this form is signed and submitted by a person other than the Participant identified above, the OHCA will require verification of the authority of the person signing on behalf of the Participant before this request will be considered complete.

Barton County Community College Organized Health Care Arrangement
Response to Request for Accounting of Disclosures of Protected Health Information

To:_____

The OHCA has received and reviewed the Request for Accounting of Disclosures of Protected Health Information. You are hereby notified that (check one):

☐ **Your Request is Incomplete.** Your request is being returned to you because it is incomplete. Your request is incomplete in the following way(s): _____

_____

_____

A new Request for Accounting of Disclosures of Protected Health Information is enclosed. Please resubmit your request.

☐ **The OHCA is Granting Your Request.** The OHCA is granting your Request. If you requested that the information be mailed to you, the information is enclosed with this letter. In the alternative, if you chose to receive the requested information in person, please call the Benefit Specialist at (620) 792-9235 during regular business hours to arrange for a mutually convenient time to receive the requested information.

☐ **The OHCA is Denying Your Request.** The OHCA is denying your Request. Your request is denied for the following reason(s):

- ☐ Your request for an accounting must be related to disclosures that occurred within the last 6 years;
- ☐ Your request for an accounting may not relate to a period prior to the effective date of HIPAA medical privacy compliance; or
- ☐ Other: _____

Complaints. If you are dissatisfied with the manner in which the OHCA has responded to your request, you may file a complaint with the OHCA and with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the OHCA, contact the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with us.

Barton County Community College Organized Health Care Arrangement
Request for Confidential Communications

You have the right to request that the Barton County Community College Organized Health Care Arrangement (the "OHCA") communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that the OHCA only contact you at work or by mail. To request confidential communications, please provide the information requested below, sign this Request and submit it in person to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, Monday through Friday during the hours of 8 a.m. and 5 p.m. In the alternative, you may submit this Request by depositing it in the United States mail, postage prepaid, and addressed to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530.

Individual Information. Please provide the following information:
Name: _____
Date of Birth: ____/____/____
Social Security Number:_____
Address: _____
Telephone Number: _____

Request for Confidential Communications. I hereby request that the OHCA communicate with me regarding my protected health information specified below in the manner and/or location specified below. As described immediately below, my request for confidential communications is necessary to prevent a disclosure that could endanger me.

Please describe why your request is necessary to prevent a disclosure that could endanger you:

_____

_____

_____

Description of Protected Health Information to be Communicated Confidentially. This Request for Confidential Communications applies to the protected health information specified below (please check one or more):

☐ Full record. ☐ Full record for the period ____/____/____ to ____/____/____.
☐ Enrollment information. ☐ Premium / contribution payment information.
☐ Claims and billing information relating to the following service or claim (specify date of service and/or medical condition): _____

_____

☐ Other (please specify):_____

_____

Alternative Manner and/or Location for Confidential Communications. Please describe how you want the protected health information specified above to be communicated to you:

_____

_____

The OHCA's Obligation. The OHCA is required to accommodate your requests if your request is reasonable and you clearly provide information that the disclosure of all or part of that information could endanger you. You will be notified by the OHCA, in writing, of the OHCA's decision regarding this Request within 60 days of your Request.

_____ _____

Signature Date

_____

Print Name

Please Note: If this form is signed and submitted by a person other than the Participant identified above, the OHCA will require verification of the authority of the person signing on behalf of the Participant before this request will be considered complete.

Barton County Community College Organized Health Care Arrangement
Response to Request for Confidential Communications

To:_____

The OHCA has received and reviewed your Request for Confidential Communications. You are hereby notified (check one):

☐ **Your Request is Incomplete.** Your request is being returned to you because it is incomplete. Your request is incomplete in the following way(s):_____
_____
_____

A new Request for Confidential Communications is enclosed. Please resubmit your request.

☐ **The OHCA is Granting Your Request.** Your Request for Confidential Communications has been granted. Until notified in writing by you, the OHCA will communicate with you regarding the protected health information specified in your Request in the manner and/or locations specified in your Request.

☐ **The OHCA is Denying Your Request.** The OHCA is denying your request. The basis for this denial is as follows: _____
_____
_____
_____
_____

Complaints. If you are dissatisfied with the OHCA's decision, you may file a complaint with the OHCA and with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the OHCA, contact the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with us.

Barton County Community College Organized Health Care Arrangement
Request for Restrictions to Protected Health Information

You have the right to request that restrictions and/or limitations be placed on your protected health information that the Barton County Community College Organized Health Care Arrangement (the "OHCA") uses or discloses about you for treatment, payment or health care operations. You also have the right to request a limit on the protected health information disclosed by the OHCA to someone who is involved in your care or the payment for your care, like a family member or friend. To request restrictions on your protected health information that the OHCA uses or discloses about you for treatment, payment or health care operations, please provide the information requested below, sign this Request and submit it in person to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, Monday through Friday during the hours of 8 a.m. and 5 p.m. In the alternative, you may submit this Request by depositing it in the United States mail, postage prepaid, and addressed to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530.

Individual Information. Please provide the following information:
Name: _____
Date of Birth: ____/____/____
Social Security Number:_____
Address: _____
Telephone Number: _____

Identification of Restricted Protected Health Information. I hereby request that the OHCA restrict the use and disclosure of the protected health information specified below (please check one or more):

☐ Full record. ☐ Full record for the period ____/____/____ to ____/____/____.
☐ Enrollment information. ☐ Premium / contribution payment information.
☐ Claims and billing information relating to the following service or claim (specify date of service and/or medical condition): _____
_____

☐ PHI pertaining solely to a health care item or service for which the health care provider has been paid out of pocket in full, where such disclosure is to another health plan for purposes of carrying out payment or health care operations.

☐ Other (please specify):_____
_____

Identification of Persons / Organization Restricted from the Use and Disclosure of Protected Health Information. I hereby request that the following persons or organizations not be allowed to use, receive and/or disclose the protected health information specified above:

_____
_____
_____

The OHCA's Obligation. The OHCA is not required to allow the restrictions and/or limitations you have requested except where the request is related to the disclosure of PHI to a health plan where the provider was paid out of pocket in full, as described above. You will be notified by the OHCA, in writing, of the OHCA's decision regarding this Request. Generally, the OHCA is required by law to act on this Request within 60 days of the receipt. The OHCA is not required to agree to your requested restrictions.

_____ _____

Signature Date

_____

Print Name

Please Note: If this form is signed and submitted by a person other than the Participant identified above, the OHCA will require verification of the authority of the person signing on behalf of the Participant before this request will be considered complete.

Barton County Community College Organized Health Care Arrangement
Response to Request for Restrictions to Protected Health Information

To:_____

The OHCA has received and reviewed your Request for Restrictions to Protected Health Information. You are hereby notified (check one):

☐ **Your Request is Incomplete.** Your request is being returned to you because it is incomplete. Your request is incomplete in the following way(s):_____
_____
_____

A new Request for Restrictions to Protected Health Information is enclosed. Please resubmit your request.

☐ **The OHCA is Granting Your Request.** The OHCA agrees to the restrictions on the use and/or disclosure of protected health information you requested. The restrictions on the use and/or disclosure of protected health information you requested will be maintained as part of your protected health information for so long as the OHCA holds those records. Until your requested restrictions are revoked or terminated (see below), the OHCA may not use or disclose your protected health information in violation of your requested restrictions, except in emergency situations or to public health, governmental, or law enforcement officials with proper documentation.

☐ **The OHCA is Denying Your Request.** The OHCA is denying your request. The basis for this denial is as follows: _____
_____
_____
_____

Termination of Restrictions by the OHCA. The OHCA may, at any time, inform you that it is terminating its agreement to abide by your requested restrictions and, after notifying you of its decision, may use or disclose your protected health information in the manner provided by law.

Revocation of Restrictions. You have the right to cancel the restrictions granted by the OHCA at any time. Your revocation of the restrictions granted by the OHCA must be in writing, must be signed by you and must indicate the specific restrictions you wish to revoke. For example, your written revocation might identify the restrictions to be revoked with reference to the date your Request for Restrictions to Protected Health Information was submitted or with reference to the person or organization to whom your Request for Restrictions to Protected Health Information applied to. You may submit your revocation in person to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530, Monday through Friday during the hours of 8 a.m. and 5 p.m. In the alternative, you may submit this Authorization by depositing it in the United States mail, postage prepaid, and addressed to the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530.

Complaints. If you are dissatisfied with the OHCA's decision, you may file a complaint with the OHCA and with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the OHCA, contact the Benefit Specialist, 245 NE 30, Great Bend, Kansas 67530. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with us.

Barton County Community College Organized Health Care Arrangement
Disclosure Report Form

A. Purpose of Form

HIPAA requires that uses and disclosures of protected health information be documented. To that end, the OHCA has adopted policies and procedures that require all disclosures of protected health information to be documented on this Disclosure Report form.

B. Instructions

For each disclosure of an individual's protected health information, excluding disclosures made to Barton County Community College, complete the following and file the completed form, together with copies of any documents associated with the disclosure, including authorizations and requests submitted by individuals and the OHCA's response thereto, in the individual's file.

1. Name of individual whose protected health information was disclosed:_____
   _____

2. Date of the disclosure: _____

3. The name of the entity or person who received the protected health information and, if known, the address of that entity or person: _____
   _____
   _____

4. Provide a brief description of the information disclosed: _____
   _____
   _____

5. Provide a brief statement of the purpose of the disclosure: _____
   _____
   _____

6. In the space below, list all documents associated with the disclosure and attach copies of the same: _____
   _____
   _____

This Disclosure Report was prepared by _____ on _____.

_____
Signature of Authorized Employee

Barton County Community College Organized Health Care Arrangement
Employee Training Log

The HIPAA privacy regulations require employer-sponsored group health plans to protect protected health information against unauthorized use or disclosure. To that end, the employer, in its capacity as the plan sponsor, is responsible for training all members of its workforce on its privacy policies and procedures.

Employee Name	Date of Training	Trained By	Form of Training	Employee Acknowledgment

Employee Name	Date of Training	Trained By	Form of Training	Employee Acknowledgment

Barton County Community College Organized Health Care Arrangement
Employee Acknowledgment

Employee's Name:_____

This document certifies that the person named above has satisfactorily completed the training specified immediately below which is required in conjunction with the compliance efforts of the Barton County Community College Organized Health Care Arrangement (the "OHCA") and Barton County Community College (the "Employer") with the medical privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"):

Please describe the specific training provided and the date it was provided._____

_____

_____

_____

By signing this Employee Acknowledgment, the above named employee certifies to the OHCA and the Employer the following:

(1) I have received the HIPAA training described above on the date indicated;

(2) In connection with my HIPAA training:

☐ I was provided a copy of the OHCA's HIPAA Privacy Policy and Procedures; or

☐ I reviewed a copy of the OHCA's HIPAA Privacy Policy and Procedures;

(3) I have read, understand and agree to abide by the policies and procedures in the OHCA's HIPAA Privacy Policy and Procedures;

(4) I have been given an opportunity to ask any and all questions that I have in regards to the OHCA's HIPAA Privacy Policy and Procedures, and how the same applies to the performance of my employment responsibilities; and

(5) I understand and acknowledge that the penalties for not following the OHCA's HIPAA Privacy Policy and Procedures can be severe, including termination.

Employee's Signature: _____
Print Name: _____
Date: _____

Barton County Community College Organized Health Care Arrangement
HIPAA Security Compliance
- Risk Analysis Worksheet -

You will need to complete a separate worksheet for each group health plan that you sponsor. If, however, your group health plans are part of an "organized health care arrangement" ("OHCA"), you may complete one worksheet for the OHCA.

Enter the full legal name of the OHCA to which this analysis applies:

Name of OHCA: Barton County Community College Organized Health Care Arrangement

Background

In deciding whether or not to implement certain security measures to protect electronic PHI or "e-PHI," the following is being considered:

- The size, complexity, and capabilities of the OHCA.
- The technical infrastructure, hardware and software capabilities of the OHCA.
- The costs of security measures.
- The probability and criticality of potential risks to e-PHI.

Compliance Tips

- *This documentation should be retained for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.*
- *This document should be periodically reviewed and updated as necessary.*

Please answer the following questions in order to analyze and document the risk that e-PHI might be used or disclosed by unauthorized parties.

(1) ***Does the OHCA have any of the following?*** *(Check if applicable)*

Employees	□	Yes	□	No
Computer Hardware	□	Yes	□	No
Computer Software	□	Yes	□	No
Facilities *(such as its own worksite)*	□	Yes	□	No

Compliance Tip

Most group health plans are "virtual" entities. That is, they are little more than a piece of paper. They do not need their own employees, hardware, etc. in order to exist, but they do need someone to act on their behalf. Our guess is that you will answer "no" to the above categories.

If you checked "yes" to any of the above, please describe who or what makes up the above categories in the lines that follow. You will need to consult legal counsel to determine what security obligations exist for the OHCA. The cost of compliance, the size of the plan, etc. will be taken into consideration in determining your compliance requirements:

_____

_____

_____

If you checked "no" for each category above because the OHCA exists in the form of a document only and, thus, has no employees, hardware, etc., please continue to Question (2).

(2) ***Are you (as an employer-plan sponsor) already in compliance with the HIPAA medical privacy rules? Specifically, have you already set up administrative, physical and technical safeguards to protect PHI?***

□ Yes

□ No

If "yes," most of your security obligations are completed because many of the security requirements dovetail the privacy requirements. Continue to Question (3).

If "no," please check the reason below for not already being in compliance with the HIPAA medical privacy rules:

□ **Exception under HIPAA Medical Privacy.** Your OHCA falls within the limited exception of being a self-funded, self-administered plan with less than fifty (50) eligible employees. This means the OHCA was not subject to the HIPAA medical privacy rules. The OHCA, however, does create, maintain, transmit or receive e-PHI so it must comply with the HIPAA security rules. It may be helpful for you to complete the Technical and Physical Safeguard Worksheet found elsewhere in the HIPAA Handbook to analyze where PHI is found in your organization, by whom, and what you can do to protect it. This will help you ensure that any e-PHI is reasonably and adequately protected. Once this is done, you should continue to Question (3).

□ **HIPAA Lite.** Your OHCA is in "HIPAA Lite." This means the only health information it sees is "summary health information" and/or "enrollment / disenrollment" information. This OHCA, although subject to HIPAA medical privacy, has very limited HIPAA privacy obligations. For this reason, there was no need to set up administrative, physical and technical safeguards. In addition, the security rules do not apply to "summary health information" and/or "enrollment / disenrollment" information even if it is received in electronic form. Please skip to Conclusion B at the end of this worksheet and check the box.

If you do not fit within one of the above reasons, then you have no excuse for not complying with HIPAA medical privacy up until now! Your OHCA should be in compliance with HIPAA medical privacy and you should take immediate action to set up administrative, physical and technical safeguards as part of the HIPAA privacy compliance process. This will also act as a first step toward security compliance. You should stop this risk analysis now and begin it again when you have finished your HIPAA medical privacy compliance.

(3) ***Have you amended your plan document(s) for HIPAA security?***

□ Yes

□ No

If "yes," continue to Question (4).

If "no," the security regulations require group health plans to be amended to require, among other things, the plan sponsor to protect e-PHI that it creates, receives, maintains, or transmits on behalf of the group health plan. You should have your plan document(s) amended by April 20, 2005 (applies to "large" plans) or April 20, 2006 (applies to "small" plans). Once the plan documents have been amended, please continue to Question (4) and proceed with this analysis.

(4) ***Does the OHCA have any business associates?***

□ Yes

□ No

If "yes," continue to Question (5).

If "no," you do not need to amend any business associate agreements. Please skip to Conclusion A at the end of this worksheet and check the box.

(5) ***Have you amended your business associate agreement(s) for HIPAA security?***

□ Yes

□ No

If "yes," list each business associate agreement which has been amended:

_____

_____

By amending the above agreements so that business associates may act on behalf of the OHCA, your security obligations have been reduced. The OHCA itself will not have e-PHI to create, maintain, transmit or receive since the business associate (or the plan sponsor) will do so on the OHCA's behalf. Please skip to Conclusion A at the end of this worksheet and check the box.

If "no," list the business associate agreement(s) that you have not amended and explain why:

_____

_____

The OHCA will not be able to share e-PHI with the above business associates. Please skip to Conclusion A at the end of this worksheet and check the box.

From the above analysis, which has been conducted on behalf of the OHCA, we have concluded the following:

Conclusion A.

□ The potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by OHCA is very low due to the fact that the OHCA has no employees, no hardware, no software, and no premises or facilities. Any e-PHI is, therefore, in the hands of the employer/plan sponsor and/or business associates of the OHCA. Consequently, the plan document has been amended to reflect the plan sponsor's security obligations and any business associate agreements have been amended to reflect the security obligations of the business associates who will create, maintain, transmit, or receive e-PHI on behalf of the OHCA.

Conclusion B.

□ The OHCA does not create, transmit, maintain, or receive e-PHI other than "summary health information" and/or "enrollment / disenrollment" information. Consequently, there is no need to amend the plan documents at this time to reflect that e-PHI will be reasonably and adequately protected as required under the security rules.

Completed on this _____ day of _____, 20____.

By: _____*(Signature)*

Print Name: _____

Title: Security Officer

Barton County Community College Organized Health Care Arrangement
Breach Determination – Risk Assessment

Please complete Steps One through Four, as necessary, in order to document your analysis of whether a Breach of Unsecured PHI has occurred.

What is a Breach? A Breach is the acquisition, access, use, or disclosure of PHI in an impermissible manner that compromises the security or privacy of the PHI (see Policies and Procedures for a more detailed definition, including three specific exceptions to the definition of a Breach).

Name of OHCA: Barton County Community College Organized Health Care Arrangement

Step One: Determine whether the PHI was "unsecured." If the PHI that was used or disclosed in an impermissible manner was not encrypted in accordance with HHS guidance, it is "unsecured" PHI. *Please check the appropriate box below and follow the instructions.*

☐ **PHI Was Encrypted.** *Please proceed to Step 6. The PHI is "secured" and cannot be "breached." Please attach proof or documentation that PHI was encrypted.*

☐ **PHI Was Not Encrypted.** *Please proceed to Step 2.*

Step Two: Determine whether the PHI was used or disclosed in an unauthorized manner. The Policies and Procedures set forth all required and permissible uses and disclosures of PHI. Please review the Policies and Procedures and then indicate whether the use or disclosure was authorized or unauthorized.

☐ **Use or Disclosure of PHI was Permissible.** The PHI was used or disclosed as follows and such use or disclosure is permissible as set forth in the Policies and Procedures:

_____

_____

☐ **Use or Disclosure of PHI was not Permissible.** The PHI was used or disclosed as follows and such use or disclosure is not a permissible use or disclosure set forth in the Policies and Procedures:

_____

_____

_____

If the use or disclosure was permissible, proceed to Step 6; if the use or disclosure was impermissible, proceed to Step 3.

<u>Step Three</u>: Determine and document whether the impermissible use or disclosure compromises the privacy or security of PHI. The acquisition, access, use, or disclosure of PHI in an impermissible manner is presumed to be a breach unless you can demonstrate that there is a low probability that the PHI has been compromised. Such a demonstration must be based on a risk assessment that includes the following factors:

- *The unauthorized person who used the PHI or to whom the disclosure was made.*

  Example. The PHI was impermissibly disclosed to another entity governed by the HIPAA privacy and security rules. Therefore, there is a low probability that the PHI was compromised because the recipient entity is already obligated to protect the privacy or security of the information it received in the same manner as the OHCA.

- *The extent to which the risk to the PHI has been mitigated.*

  Example. There is a low probability that the PHI was compromised because the OHCA immediately obtained satisfactory assurances from the recipient that the information will not be further used or disclosed or that it will be destroyed. A confidentiality agreement was signed.

- *Whether the PHI was actually acquired or viewed.*

  Example. A laptop with PHI was lost and then recovered. It can be shown that the information on the laptop was not opened, altered, or transferred, so the OHCA does not believe that the PHI was viewed and, therefore, the PHI was not compromised.

- *The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.*

  Example One. The PHI that was improperly disclosed does not include the name, date of birth, zip code, or any other identifying information of the individual, nor does it reveal the fact that the individual received services from a hospital. Accordingly, we believe that there is a low probability that PHI has been compromised.

  Example Two. The PHI that was improperly disclosed indicates that the individual received services from a specialized facility (such as a substance abuse treatment program). Therefore, we believe that there is more than a low probability that PHI has been compromised.

  Example Three. The PHI that was improperly disclosed includes information that increases the risk of identity theft (such as a Social Security number and/or mother's maiden name). Therefore, we believe that there is a high probability that PHI has been compromised.

  _____

  _____

  _____

  _____

- *Other Factor(s):* _____

  Explain how this factor(s) supports or does not support the notion that the use or disclosure of the PHI has compromised the privacy or security of the PHI:

  _____

  _____

  _____

Based on the factors above, indicate whether the impermissible use or disclosure compromises the privacy or security of PHI by <u>checking the appropriate box below</u>:

☐ The privacy and/or security of PHI was compromised. *Proceed to Step 4.*

☐ The privacy and/or security of PHI was <u>not</u> compromised and, consequently, there is no Breach of Unsecured PHI. *Proceed to Step 6.*

Step Four: Determine whether the incident falls under one of the three exceptions to the Breach definition. If you have determined that there was a "breach," you now need to determine if the "breach" in question falls within one of three exceptions to the Breach definition in the privacy and security regulations. Read each exception below. *After reading each exception, check the appropriate box next to each exception, indicating whether or not the exception applies.*

Exception 1. Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the OHCA will not constitute a Breach if such acquisition, access, or use was made in good faith and within the course and scope of employment or other professional relationship of such employee or individual with the OHCA, and the information is not further acquired, accessed, used, or disclosed by any person in a manner not permitted by the Privacy and/or Security Rules.

> *Example of Exception 1.* An employee in the HR department receives and opens an email containing PHI about a plan participant. The email should have been sent to a colleague who handles the benefits side of HR. The employee notices that he is not the intended recipient, alerts the sender of the misdirected email, and then deletes the email. The employee unintentionally accessed PHI to which he was not authorized to have access. However, this was done in good faith and within the scope of authority. No breach notification is required because this is not a Breach.

Is this Exception 1 satisfied?

☐ If "yes," there is no "Breach." Explain: _____

Proceed to Step 6.

☐ If "no," *proceed to Exception 2.*

Exception 2. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by the OHCA to another similarly situated individual at the same facility will not constitute a Breach so long as the information received is not further used or disclosed in a manner not permitted by the Privacy and/or Security Rules.

> *Example of Exception 2.* One authorized employee inadvertently leaves a fax containing PHI on another authorized employee's desk. The second employee reads the fax before realizing that the fax was not intended for her. She returns the fax to the first employee and does not further use or disclose the PHI. No breach notification is required because this is not a Breach.

Is this Exception 2 satisfied?

☐ If "yes," there is no "Breach." Explain: _____

_____

Proceed to Step 6.

☐ If "no," *proceed to Exception 3.*

Exception 3. Any disclosure to an unauthorized person will not constitute a Breach where there is a good faith belief that the PHI that was disclosed would not reasonably have been retained by such person.

> *Example of Exception 3.* The OHCA sends a number of EOBs to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. The OHCA concludes that the recipients of the EOBs could not reasonably have retained the information since the envelopes were returned unopened. However, the EOBs that were not returned as undeliverable and that the OHCA knows were sent to the wrong individuals should be treated as Breaches.

Is this Exception 3 satisfied?

☐ If "yes," there is no "Breach." Explain: _____

_____

Proceed to Step 6.

☐ If "no," *proceed to Step 5.*

---- Breach Determination -----

Step Five: Breach of Unsecured PHI. It has been determined that there has been a Breach of Unsecured PHI based on the risk assessment completed above. *Each of the following steps below should be followed:*

☐ **Documentation.** This risk assessment shall be kept in the records of the OHCA.

☐ **Notifications.** The appropriate parties (individuals, HHS, and, if necessary, the media) will be notified in accordance with the Policies and Procedures).

☐ **Log.** The "Log of Breaches of Unsecured PHI" form shall be completed. This is Exhibit 18 and is part of the Policies and Procedures.

Proceed to Step 7.

Step Six: No Breach of Unsecured PHI. It has been determined that there has not been a Breach of Unsecured PHI for the following reason *(check the appropriate box)*:

☐ **Encryption.** The PHI was encrypted and, consequently, there was no Breach of Unsecured PHI. Proof or documentation of encryption is attached.

☐ **Permissible Use or Disclosure.** There was no Breach of Unsecured PHI because the PHI was used or disclosed in a manner which is permissible under the HIPAA medical privacy and security regulations and as reflected in the Policies and Procedures of the OHCA.

☐ **Privacy and/or Security of PHI Not Compromised.** Although PHI was acquired, accessed, used, or disclosed in an impermissible manner, there is no Breach of such PHI because the privacy and /or security of the PHI was not compromised.

☐ **Breach Exception.** Although the breach meets the basic definition of a Breach of Unsecured PHI, this particular incident falls within one of the exceptions to the definition of a Breach and, consequently, there is no Breach of Unsecured PHI.

Keep this Risk Assessment in the records of the OHCA for 6 years in accordance with the OHCA's Policies and Procedures. Proceed to Step 7.

Step Seven: Certification.

I hereby certify that I have completed this Risk Assessment to the best of my knowledge and have made the determination as indicated in either Step 5 or Step 6 above.

Signature: _____

Print Name: _____

Title: _____

Date: _____

Barton County Community College Organized Health Care Arrangement

Log of Breaches of Unsecured Protected Health Information ("PHI")

Any time the OHCA discovers a Breach of Unsecured PHI, the OHCA has reporting obligations to the Secretary of Health and Human Services ("HHS"). For Breaches involving 500 or more individuals, the OHCA will consult with the HHS website for immediate notification requirements. For Breaches involving fewer than 500 individuals, information regarding each Breach shall be kept using this Log of Breaches of Unsecured PHI.

Specific Name of the OHCA Involved in the Breach	**Date of Breach**	**Date of Discovery of Breach**	**Number of Individuals Affected by the Breach**	**Type of Breach**	**Identity of Unauthorized User or Recipient of PHI**	**Type of PHI**	**Protective Measures in Place Prior to Breach**	**Date(s) Individual Notice(s) Sent**	**Did Any Individual Require the Use of a "Substitute" Notice?**	**Was PHI actually acquired or viewed?**	**Brief Description of What Happened (Include Location of PHI at Time of Breach)**
Example(s):											
ABC Company LLC Medical Plan	*11/30/21*	*12/03/21*	*1*	*Theft, loss, improper disposal, unauthorized access, hacking/IT incident, other*	*Another covered entity, a business associate, a criminal*	*Demographic, financial, clinical, other*	*Firewalls, packet filtering (router-based), secure browser sessions, strong authentication, encrypted wireless, physical security, antivirus software, biometrics, intrusion detection*	*12/15/21*	*No*	*No*	*Laptop stolen out of Employee's car. Police contacted and report filed.*

CONTENTS

Organized Health Care Arrangement Designation Form (Form 500) 1

Hybrid Entity Designation Form (Form 505) 2

Privacy Officer Designation and Acceptance Form (Form 510) 3

Security Officer Designation and Acceptance Form (Form 511) 4

Contact Person Designation and Acceptance Form (Form 515) 5

Technical and Physical Safeguard Worksheet (Form 520) 6

HIPAA Privacy & Security Safeguard - Checklist 7

Business Associate Worksheet (Form 525) 8

Barton County Community College Organized Health Care Arrangement

Miscellaneous Administrative Forms

HINKLE LAW FIRM LLC

Barton County Community College Medical, Dental, and Prescription Plan
Barton County Community College Level II Preventive Health Benefits Plan
Barton Community College Health Flexible Spending Account
- Organized Health Care Arrangement ("OHCA") Designation Form -

The following group health plans, all of which are sponsored by Barton County Community College, do hereby form an "organized health care arrangement" for the purpose of complying with the HIPAA medical privacy regulations:

Plan #1 Barton County Community College Medical, Dental, and Prescription Plan

Plan #2 Barton County Community College Level II Preventive Health Benefits Plan

Plan #3 Barton Community College Health Flexible Spending Account

The organized health care arrangement formed by the above named group health plans shall be known as the Barton County Community College Organized Health Care Arrangement (the "OHCA").

The undersigned group health plans (referred to individually herein as the "Plan") hereby individually certify that (i) Barton County Community College is the sponsor of the OHCA; (ii) the OHCA shall share all policies, procedures, forms and other documents required to comply with the HIPAA medical privacy regulations with the other members of the OHCA; and (iii) the OHCA shall treat the policies, procedures, forms and other documents required to comply with the HIPAA medical privacy regulations issued by the OHCA, as well as any other HIPAA compliance efforts made by the OHCA, as its own and hereby agrees to be bound by the same.

This OHCA Designation is signed and agreed to this ____ day of _____, 20__.

_____
Barton County Community College

_____
Barton County Community College Medical, Dental, and Prescription Plan

_____
Barton County Community College Level II Preventive Health Benefits Plan

_____
Barton Community College Health Flexible Spending Account

Barton Community College Flexible Benefit Plan
- Hybrid Entity Designation -

The Barton Community College Flexible Benefit Plan (the "Plan"), which is sponsored by Barton County Community College ("Employer"), is a "hybrid entity" for purposes of the HIPAA medical privacy regulations. As such, the plan is made up of both health care and non-health care benefits. This Hybrid Entity Designation is made for the purpose of identifying and designating that part of the plan that is a "group health plan" for purposes of the HIPAA medical privacy regulations (being referred to herein as the "Plan") and that part of the plan that is not.

The Plan hereby designates the following benefits as constituting the Plan for purposes of the HIPAA medical privacy regulations:

Barton County Community College Medical, Dental, and Prescription Plan
Barton County Community College Level II Preventive Health Benefits Plan
Barton Community College Health Flexible Spending Account

All other benefits provided by the Employer through the Barton Community College Flexible Benefit Plan are either (1) not "group health plans" as defined by HIPAA or (2) provided solely through an insurance contract with a health insurance issuer or HMO and do not create or receive protected health information other than enrollment or disenrollment information, or "summary health information" as defined in 42 C.F.R. Section 164.504(a).

In addition to making the required election, the HIPAA medical privacy regulations require that a hybrid entity implement safeguards to ensure that protected health information is not disclosed by the health care component of the hybrid entity (the Plan) to the other non-health care component(s) of the hybrid entity. To that end, the Plan shall adopt and implement policies and procedures to ensure the privacy and protection of protected health information in the manner required under the HIPAA medical privacy regulations.

This Hybrid Entity Designation is signed and agreed to this _____ day of _____, 20___.

_____
Barton County Community College

_____
Barton County Community College Medical, Dental, and Prescription Plan

_____
Barton County Community College Level II Preventive Health Benefits Plan

_____
Barton Community College Health Flexible Spending Account

Barton County Community College Organized Health Care Arrangement
- Privacy Officer Designation and Acceptance Form -

Date: _____

Name: Mark Dean

Title: VP of Administration

I agree to serve as the HIPAA Privacy Officer for the Barton County Community College Organized Health Care Arrangement (the "OHCA"). As the Privacy Officer, I will be responsible for performing the following duties:

- Establish, create, maintain and implement policies and procedures setting forth the standards for protection of privacy information;
- Establish, create, maintain and implement policies and procedures setting forth the standards for information that is stored or processed electronically;
- Conduct periodic reviews and audits of policies and procedures, and the OHCA's compliance with those policies and procedures;
- Review all system-related security planning and act as a liaison to internal and external vendors and consultants;
- Communicate with the OHCA's third party administrator and system vendors to ensure that HIPAA privacy standards are met;
- Ensure that each group of employees who are authorized to access a certain amount of protected health information are limited to accessing only such authorized amount;
- Coordinate initial and on-going privacy training for all appropriate employees, contractors, alliance partners, business associates, and other appropriate third parties;
- Review business associate agreements and relationships to ensure that they meet HIPAA's standards;
- Establish and oversee a process for receiving, documenting, tracking, and responding to the exercise of HIPAA rights by individuals;
- Establish and oversee a process for receiving, documenting, tracking, investigating, and taking action on all grievances and complaints concerning the OHCA's privacy policies and procedures;
- Establish appropriate sanctions for violations of the OHCA's policies and procedures and ensure that such sanctions are consistently applied to all appropriate staff and business associates;

- Serve as the OHCA's HIPAA privacy resource;
- Understand and stay current on applicable federal and state privacy laws; and
- Cooperate with the Department of Health and Human Services Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.

I have read and understand the above Privacy Officer job description. I understand that I will serve as the Privacy Officer for the OHCA at the discretion of the OHCA.

_____

Signature of Privacy Officer

Barton County Community College Organized Health Care Arrangement
- Security Officer Designation and Acceptance Form -

Date: _____

Name: Mark Dean

Title: VP of Administration

I agree to serve as the HIPAA Security Officer for the Barton County Community College Organized Health Care Arrangement (the "OHCA"). As the Security Officer, I will be responsible for performing the following duties:

- Establish, create, maintain and implement policies and procedures setting forth the standards for information that is stored or processed electronically;
- Conduct periodic reviews and audits of policies and procedures, and the OHCA's compliance with those policies and procedures;
- Ensure the confidentiality, integrity, and availability of all electronic Protected Health Information that the OHCA creates, receives, maintains, or transmits as required by the security rule;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the security rule;
- Ensure that the OHCA's workforce is in compliance with the security rule;
- Review business associate agreements and relationships to ensure that they meet HIPAA's standards;
- Establish appropriate sanctions for violations of the OHCA's policies and procedures and ensure that such sanctions are consistently applied to all appropriate staff and business associates; and
- Cooperate with the Department of Health and Human Services Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.

I have read and understand the above Security Officer job description. I understand that I will serve as the Security Officer for the OHCA at the discretion of the OHCA.

_____
Signature of Security Officer

Barton County Community College Organized Health Care Arrangement
- Contact Person Designation and Acceptance Form -

Date: _____

Name: Rebecca Jamieson

Title: Benefit Specialist

I agree to serve as the HIPAA Contact Person for the Barton County Community College Organized Health Care Arrangement (the "OHCA"). As the Contact Person, I will be responsible for performing the following duties:

- Receive and respond to requests and questions from plan participants, such as requests for information or forms;
- Receive complaints from plan participants and process those complaints in accordance with the policies and procedures established by the plan sponsor;
- Coordinate and support the efforts of the Privacy Officer to ensure that all HIPAA privacy related efforts are organized and efficient; and
- Perform other duties as delegated by the Privacy Officer.

I have read and understand the above Contact Person job description. I understand that I will serve as the Contact Person for the OHCA at the discretion of the OHCA.

_____
Signature of Contact Person

Barton County Community College Organized Health Care Arrangement
Technical and Physical Safeguard Worksheet

Authorized Employee Determination

1. Please list the names or titles in the space provided below of anyone whom you think might potentially touch protected health information.

2. Underneath the name of each individual you have listed, check the box beside each type of location where protected health information might be found (either on a temporary or permanent basis).

3. For each location listed where protected health information might be found, indicate by checking "yes" or "no" whether access to the information is available at that location.

---

a. _____
(Name / title of Privacy Officer)

___	Desk	___ Yes ___ No
___	Computer	___ Yes ___ No
___	Files and File Cabinet	___ Yes ___ No
___	Incoming / Outgoing Mail	___ Yes ___ No
___	Incoming / Outgoing Facsimiles	___ Yes ___ No
___	Other _____	___ Yes ___ No
___	Other _____	___ Yes ___ No

b. _____
(Name / title of Contact Person)

___	Desk	___ Yes ___ No
___	Computer	___ Yes ___ No
___	Files and File Cabinet	___ Yes ___ No
___	Incoming / Outgoing Mail	___ Yes ___ No
___	Incoming / Outgoing Facsimiles	___ Yes ___ No
___	Other _____	___ Yes ___ No
___	Other _____	___ Yes ___ No

c. _____

(Name / title of Other Individual Who Might Potentially Touch Protected Health Information)

___	Desk	___ Yes ___ No
___	Computer	___ Yes ___ No
___	Files and File Cabinet	___ Yes ___ No
___	Incoming / Outgoing Mail	___ Yes ___ No
___	Incoming / Outgoing Facsimiles	___ Yes ___ No
___	Other _____	___ Yes ___ No
___	Other _____	___ Yes ___ No

Do you still want the above individual to have access to protected health information?
___ Yes ___ No

d. _____

(Name / title of Other Individual Who Might Potentially Touch Protected Health Information)

___	Desk	___ Yes ___ No
___	Computer	___ Yes ___ No
___	Files and File Cabinet	___ Yes ___ No
___	Incoming / Outgoing Mail	___ Yes ___ No
___	Incoming / Outgoing Facsimiles	___ Yes ___ No
___	Other _____	___ Yes ___ No
___	Other _____	___ Yes ___ No

Do you still want the above individual to have access to protected health information?
___ Yes ___ No

e. _____

(Name / title of Other Individual Who Might Potentially Touch Protected Health Information)

___	Desk	___ Yes ___ No
___	Computer	___ Yes ___ No
___	Files and File Cabinet	___ Yes ___ No
___	Incoming / Outgoing Mail	___ Yes ___ No
___	Incoming / Outgoing Facsimiles	___ Yes ___ No
___	Other _____	___ Yes ___ No
___	Other _____	___ Yes ___ No

Do you still want the above individual to have access to protected health information?
___ Yes ___ No

f. _____

(Name / title of Other Individual Who Might Potentially Touch Protected Health Information)

___	Desk	___ Yes ___ No
___	Computer	___ Yes ___ No
___	Files and File Cabinet	___ Yes ___ No
___	Incoming / Outgoing Mail	___ Yes ___ No
___	Incoming / Outgoing Facsimiles	___ Yes ___ No
___	Other _____	___ Yes ___ No
___	Other _____	___ Yes ___ No

Do you still want the above individual to have access to protected health information?
___ Yes ___ No

g. _____

(Name / title of Other Individual Who Might Potentially Touch Protected Health Information)

___	Desk	___ Yes ___ No
___	Computer	___ Yes ___ No
___	Files and File Cabinet	___ Yes ___ No
___	Incoming / Outgoing Mail	___ Yes ___ No
___	Incoming / Outgoing Facsimiles	___ Yes ___ No
___	Other _____	___ Yes ___ No
___	Other _____	___ Yes ___ No

Do you still want the above individual to have access to protected health information?
___ Yes ___ No

h. _____

(Name / title of Other Individual Who Might Potentially Touch Protected Health Information)

___	Desk	___ Yes ___ No
___	Computer	___ Yes ___ No
___	Files and File Cabinet	___ Yes ___ No
___	Incoming / Outgoing Mail	___ Yes ___ No
___	Incoming / Outgoing Facsimiles	___ Yes ___ No
___	Other _____	___ Yes ___ No
___	Other _____	___ Yes ___ No

Do you still want the above individual to have access to protected health information?
___ Yes ___ No

Go to Part B of the Introduction to your Policy and Procedures. The names or titles of all of the individuals identified above that you would still like to have access to protected health information should match the names or titles in Part B of the Introduction to the Policy and Procedures. These are your Authorized Employees.

Implementation of Safeguards

HIPAA requires an employer to establish, on behalf of its group health plan(s), technical and physical safeguards to prevent protected health information from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements.

In the material below, we set forth the policies and procedures to implement HIPAA's technical and physical safeguard requirements. Once you have read each policy and the corresponding procedures, please indicate how information at each type of location will be safeguarded. For example, protected health information found in or on someone's desk might be safeguarded by ensuring that each individual can lock his or her desk. Similarly, protected health information found in someone's computer might be safeguarded by ensuring that computer access is password protected.

Safeguarding Protected Health Information Received by Mail.

Policy: Protected health information received by mail may only be opened by an individual who is an Authorized Employee.

Implementation: You will need to do the following:

(1) Identify the individual or individuals who are authorized to receive protected health information by mail; and
(2) Notify all persons and/or organizations who send protected health information by mail to address all correspondence to those individuals.

Individuals who are authorized to receive protected health information by mail are as follows:

_____ _____
_____ _____
_____ _____

Individuals or organizations who send protected health information by mail and who should address all future correspondence to the above listed individuals are as follows:

_____ _____
_____ _____
_____ _____

Safeguarding Protected Health Information Received by Facsimile.

Policy: Protected health information received by facsimile may only be viewed by an individual who is an Authorized Employee.

Implementation: You will need to do the following:

(1) Identify the individual or individuals who are authorized to receive protected health information by fax;
(2) Notify all persons and organizations who send protected health information by fax to address all fax correspondence only to authorized individuals; and
(3) Provide Authorized Employees with the capability to receive faxes at their computer terminals or designate a fax machine in a secure location for the receipt of protected health information or request and require persons sending protected health information by fax that, prior to transmitting protected health information, they contact an individual authorized to receive protected health information by fax who can attend the fax machine.

Individuals who are authorized to receive protected health information by facsimile are as follows:

_____ _____
_____ _____
_____ _____

Individuals or organizations who send protected health information by facsimile and who should address all future correspondence to the above listed individuals are as follows:

_____ _____
_____ _____
_____ _____

Choose one or more of the following:

□ Individuals who are authorized to receive protected health information may be provided with the capability to receive faxes at their computer terminal. The individuals with such capabilities and their fax numbers are as follows:

_____
_____
_____

□ A fax machine in a secure location has been specifically designated for the receipt of protected health information. The designated fax machine location and number are:

_____
_____
_____

□ Prior to transmitting protected health information, the persons listed immediately above (i.e., the senders) are requested and required to contact an individual authorized to receive protected health information by fax who can attend the fax machine while the fax is being transmitted.

Safeguarding Protected Health Information Stored or Filed in Paper Format.

Policy: Designated records sets should be maintained separately and secured separately from all employee records and stored in locked filing cabinets or in a locked file room to ensure they will be safeguarded from unauthorized view. In addition, the Policy requires that access to the locked file cabinets and/or locked area be limited to Authorized Employees.

Implementation: You will need to do the following:

(1) Designate a secure location for the filing and storage of protected health information; and
(2) Limit physical access to that secure location, whether it be a desk, file cabinet or file room, to Authorized Employees.

Identify the specific secure location(s) where protected health information, and protected health information alone, will be stored, and the form of security (e.g., the locking file cabinet located in John Q. Employee's office).

_____
_____
_____
_____
_____
_____

Safeguarding Protected Health Information Received, Maintained or Stored Electronically.

Policy: Any and all protected health information received, maintained or stored on computers must be password protected with access limited to Authorized Employees. In addition, any protected health information that is received, maintained or stored electronically and that is copied onto removable media, including backup media, must be protected in the same manner as paper files.

Implementation: You will need to do the following:

(1) Identify individuals who have access to protected health information that is received, maintained or stored electronically; and
(2) Identify the form of security (e.g., password, restricted access folders, etc.) used to limit access to the information with above identified individuals.

Choose one of the following:

□ In the space provided below, identify the individual(s) who will have access to protected health information that is received, maintained or stored electronically, and the form of security (e.g., password, restricted access folders, etc.) used to limit access to the information to those individuals:

Name / Title of Individual	Form of Security
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

or

□ Protected health information is not received, maintained or stored on computers.

Choose one of the following:

Indicate below whether protected health information in electronic format is ever copied by Authorized Employees onto removable media (e.g., flash drives, USB drives, or external hard drives) or if protected health information is automatically copied through back-up procedures.

□ The media onto which protected health information is copied must be safeguarded and protected in the same manner as paper files (see the Policies above relating to the filing and storage of protected health information in paper format).

or

□ Protected health information is not received, maintained or stored on computers.

Other Physical Safeguards.

Policy: All material containing protected health information must be protected from deliberate or casual viewing by passers-by while in use by Authorized Employees. Check the box beside each of the following safeguards as appropriate to indicate which safeguards, if any, have been implemented:

□ Computer screens displaying protected health information have been turned away from public areas so as not to be visible to passers-by in public areas;

□ Files and papers containing protected health information are not left unattended and unsecured;

□ Any and all handwritten notes such as phone messages and reminder slips containing protected health information are shredded or otherwise destroyed as soon as they are no longer needed;

□ Dictation tapes containing protected health information are erased after the material is transcribed;

□ Unwanted or duplicate papers containing protected health information are shredded or otherwise destroyed immediately after it is determined that they are no longer needed;

□ Any electronic media containing protected health information is wiped when the data is no longer required;

□ Hard drives are reformatted when an office computer is sold or when Authorized Employees no longer use them to access protected health information;

□ Other:_____

_____

HIPAA Privacy & Security Safeguards - Checklist

Physical Safeguards	✓
Lock file cabinets, drawers, and doors to rooms containing PHI	
Only permit authorized employees to have access to rooms and file cabinets containing PHI	
Do not leave rooms and file cabinets containing PHI unlocked while unattended	
If rooms or file cabinets containing PHI are locked using a number code or key, change the number code or lock whenever an authorized employee leaves the company or ceases to be an authorized employee	
Maintain PHI separately from all other records (including employee personnel files)	
Place fax machines that may receive PHI in secure areas	
Shred paper containing PHI as soon as it is no longer needed	
Retain documentation (e.g., privacy notice and individual authorizations) for at least 6 years from date last in effect	
Administrative Safeguards	✓
Appoint a privacy officer, security officer & contact person	
Identify potential privacy and security risks by conducting a risk analysis and documenting the analysis	
Require individuals with access to PHI to undergo HIPAA training and require updates to HIPAA training if there are changes to the HIPAA privacy or security rules	
Develop and implement policies and procedures to document and respond to privacy and security incidents	
Adopt a policy to sanction employees who fail to comply with HIPAA policies and procedures	
Conduct ongoing monitoring and evaluation of privacy and security policies and procedures	
Ensure that the plan document has been updated to comply with the HIPAA privacy and security rules	
Ensure that business associate agreements are in place with all service providers that may have access to PHI	
Ensure that business associate agreements are compliant with the HIPAA privacy and security rules	

This checklist is designed to help you evaluate the status of your HIPAA privacy and security compliance. These safeguards relate both to physical and electronic "protected health information" ("PHI"). While all of these safeguards are "best practices," not all will apply to every employer, and the failure to implement some of these safeguards is not necessarily a violation of HIPAA. In addition, there may be safeguards, not listed here, that an employer should reasonably implement. If you have questions about your HIPAA compliance, feel free to contact our office at (316) 267-2000.

Technical Safeguards	✓
Create computer firewalls	
Encrypt all data stored on any network file servers on which PHI is (or might be) saved	
Encrypt all data stored on local hard drives of desktop PCs on which PHI is (or might be) saved	
Encrypt all data stored on any laptops and portable devices that are (or might be) used to access PHI, including access through email	
Use secure email when transmitting PHI	
Install software and/or apps that allow laptops and/or portable devices to be remotely "wiped" if lost or stolen	
Password-protect computers/mobile devices containing PHI	
Implement internal monitoring process of locations where PHI is stored/accessed to track unusual activity and unauthorized access	
Password-protect individual computer directories and folders containing PHI	
Obtain individual passwords for all authorized employees	
Implement dual/multi-factor authentication for all authorized employees electronically accessing PHI in any manner	
Cut off an authorized employee's access to PHI when he/she leaves the company or ceases to be an authorized employee	
Delete PHI stored in the memory of copy machines, fax machines, and printers	
Ensure any electronic media containing PHI is wiped when the data is no longer required	
Wipe hard drives when an office computer is sold or when it is no longer used by authorized employees to access PHI	
Implement a policy that files containing PHI only be saved to cloud-based services that are HIPAA compliant and willing to sign a Business Associate Agreement	
Position computer monitors that could display PHI away from doors or other areas where they could be seen by unauthorized individuals	
Set up computers containing PHI to log off automatically when left unattended for a set length of time	
Set up portal sessions to log off automatically when left unattended for a set length of time	
Set up strong portal passwords/change the password if there is evidence of compromise/do not allow passwords to be saved in a web browser or any third-party storage application not approved by the Company	

Prepared by Hinkle Law Firm LLC

Barton County Community College Organized Health Care Arrangement
Business Associate Worksheet

Name of Business Associate	Name of Plan	Date Relationship Began	Is there a Business Associate Agreement?	Date Business Associate Agreement Signed	Date Relationship Ended
Example 1: *The Broker Company*	*ABC Company Group Medical Plan*	*January 1, 1998*	*Yes*	*April 1, 2004*	*Ongoing*
Example 2: *The XYZ Third Party Administrator, Inc.*	*ABC Company Health Flexible Spending Plan*	*January 1, 2000*	*Yes*	*April 1, 2004*	*Ongoing*

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") is entered into on this _____day of _____, 20___, by and between _____ ("Business Associate") and the Barton County Community College Organized Health Care Arrangement (the "Plan").

WHEREAS, by virtue of the services that Business Associate performs for the Plan, Business Associate is a "business associate" as that term is defined in the Privacy Rule (as defined below);

WHEREAS, in connection with Business Associate's provision of services, the Plan may disclose Protected Health Information (as defined below) to Business Associate; and

WHEREAS, as required pursuant to the final regulations promulgated under the Health Insurance Portability and Accountability Act of 1996, Business Associate agrees to undertake certain responsibilities as required by those regulations and this Agreement.

NOW, THEREFORE, it is agreed as follows:

1. **Definitions.** When used in this Agreement and capitalized, the following terms have the following meanings:

   (a) **"Breach"** shall have the same meaning as the term "breach" in 45 C.F.R. 164.402, limited with respect to Protected Health Information.

   (b) **"Breach Notification Rule"** shall mean the Standards and Implementation Specifications for Notifications of Breaches of Unsecured Protected Health Information under 45 C.F.R. Parts 160 and 164, subparts A and D.

   (c) **"Business Associate"** shall have the same meaning as the term "business associate" in 45 C.F.R. 160.103 and shall include all successors and assigns, agents, affiliates, subsidiaries (as applicable), and related companies of the Business Associate identified in the opening paragraph of this Agreement.

   (d) **"Discovery"** shall mean the first day on which such specified fact or condition (e.g., a Breach) is known to the applicable person, or, by exercising reasonable diligence would have been known to the applicable person. A person shall be deemed to have knowledge of a specified fact or condition (e.g., a Breach) if such fact or condition is known, or by exercising reasonable diligence would have been known, to any person, other than the person causing or committing the fact or condition, who is an agent of the applicable person (determined in accordance with the federal common law of agency).

   (e) **"EDI Rule"** shall mean the Standards for Electronic Transactions as set forth at 45 C.F.R. Parts 160, Subpart A and 162, Subpart A and I through R.

   (f) **"Electronic Protected Health Information"** or **"EPHI"** shall have the same meaning as the terms "Electronic Protected Health Information" or "E-PHI" in 45 C.F.R. 160.103, limited to the information created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity.

(g) **"Enforcement Rule"** shall mean the Enforcement Provisions set forth in 45 C.F.R. Part 160.

(h) **"Genetic Information"** shall have the same meaning as the term "genetic information" in 45 C.F.R. 160.103.

(i) **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996.

(j) **"HIPAA Rules"** mean the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.

(k) **"HITECH Act"** shall mean the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009.

(l) **"Individual"** shall have the same meaning as the term "Individual" in 45 C.F.R. 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. 164.502(g).

(m) **"Privacy Rule"** shall mean the Standards for Privacy of Individual Identifiable Health Information as set forth at 45 C.F.R. Part 160 and 164 Subparts A and E.

(n) **"Protected Health Information" or "PHI"** shall have the same meaning as the term "protected health information" in 45 C.F.R. 160.103, limited to the information created or received by Business Associate from or on behalf of the Plan.

(o) **"Required by Law"** shall have the same meaning as the term "required by law" in 45 C.F.R. 164.103.

(p) **"Secretary"** shall mean the Secretary of the Department of Health and Human Services or his/her designee.

(q) **"Security Incident"** shall have the same meaning as the term "security incident" in 45 C.F.R. 164.304.

(r) **"Security Rule"** shall mean the Security Standards and Implementation Specifications in 45 C.F.R. Part 160 and Part 164, subpart C.

(s) **"Subcontractor"** shall have the same meaning as the term "subcontractor" in 45 C.F.R. 160.103.

(t) **"Transaction"** shall have the same meaning as the term "transaction" in 45 C.F.R. 160.103.

(u) **"Unsecured Protected Health Information"** means Protected Health Information that is not secured through the use of technology or methodology specified by the Secretary of Health and Human Services through guidance issued by the Secretary.

Terms used, but not defined, in this Agreement shall have the same meaning as those terms in 45 C.F.R. 164.103 and 164.501.

2. **Obligations and Activities of Business Associate Regarding Protected Health Information.**

(a) **Limited Use of PHI.** Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required by Law.

(b) **Appropriate Safeguards.** Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement. Business Associate will implement administrative, physical, and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the Plan as required by the Security Rule.

(c) **Agents and Subcontractors.** Business Associate agrees to enter into a contractual arrangement with any agent and/or Subcontractor to whom it provides Protected Health Information received from the Plan (or created or received by Business Associate on behalf of the Plan), and agrees that such contractual arrangement shall incorporate the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such Protected Health Information. Business Associate agrees that such contractual arrangement shall provide that any such agent and/or Subcontractor agrees to implement reasonable and appropriate safeguards to protect the Plan's Protected Health Information. Business Associate agrees that such contractual arrangement shall provide that, in the event that a possible breach occurs with respect to the Plan's Protected Health Information, the agent and/or Subcontractor shall immediately and directly notify the Plan of such possible breach. Business Associate agrees, to the extent permitted by law, to accept full legal responsibility for any such breach that occurs as a result of its own actions or inactions and/or the actions or inactions of its agents and/or Subcontractors.

(d) **Access to PHI.** Business Associate agrees to provide access at the request of the Plan, and in the time and manner designated by the Plan, or as directed by the Plan, to an Individual in order for the Plan to meet the requirements under 45 C.F.R. 164.524.

(e) **Amendments to PHI in Designated Record Set.** Business Associate agrees to make any amendments to Protected Health Information in a Designated Record Set that the Plan directs or agrees to pursuant to 45 C.F.R. 164.526 at the request of the Plan or an Individual, and in the time and manner designated by the Plan. If the Plan requests an electronic copy of Protected Health Information that is maintained electronically in a Designated Record Set in the Business Associate's custody or control, Business Associate will provide an electronic copy in the form and format specified by the Plan if it is readily producible in such format; if it is not readily producible in such format, Business Associate will work with the Plan to determine an alternative form and format that will enable the Plan to meet its electronic access obligations under 45 C.F.R. 164.524.

(f) **Availability of Business Associate's Internal Documents Relating to Handling of PHI.** Business Associate agrees to make internal practices books and records, including policies and procedures relating to the use and disclosure of Protected Health Information available to the Plan, or, at the request of the Plan, to the Secretary, in a time and manner designated by the Plan or Secretary for purposes of the

Secretary determining the Plan's compliance with the Privacy Rule. Business Associate shall immediately notify the Plan upon receipt or notice of any request by the Secretary to conduct an investigation with respect to Protected Health Information received from the Plan and to provide to the Plan copies of any and all information provided by Business Associate to the Secretary in connection with any such investigation.

(g) **Documentation of PHI Disclosures.** Business Associate agrees to document any disclosures of Protected Health Information and information related to such disclosures as would be required for the Plan to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528. Business Associate agrees to maintain the disclosure information for at least six years following the date of the accountable disclosure.

(h) **Information Regarding PHI Disclosures.** Business Associate agrees to provide to the Plan or an Individual, in a time and manner designated by the Plan, information collected in accordance with paragraph (g) above of the Agreement, and to permit the Plan to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528.

(i) **Use of PHI Consistent with Plan's Intent.** Business Associate agrees to use or disclose Protected Health Information pursuant to the request of the Plan; provided, however, that the Plan shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by the Plan.

(j) **Limited Disclosures of PHI Involving Fully-Paid Out-of-Pocket Expenses.** Business Associate agrees to restrict the disclosure of PHI of a Plan participant (unless the disclosure is otherwise required by law) if the participant so requests, where the disclosure is for purposes of carrying out payment or health care operations (and not treatment) and the PHI for which the participant requests a restriction on its disclosure pertains to a health care item or service for which the health care provider has been paid out-of–pocket, in full.

(k) **Prohibition on Sale of PHI.** Business Associate shall not engage in any sale (as defined in the HIPAA Rules) of Protected Health Information.

(l) **Prohibition on Use or Disclosure of Genetic Information.** Business Associate shall not use or disclose Genetic Information for underwriting purposes in violation of the HIPAA rules.

(m) **Penalties for Noncompliance.** Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the HIPAA Rules, to the extent provided by the HITECH Act and the HIPAA Rules.

(n) **Not an Agent.** Business Associate agrees that it is an independent contractor and not an agent of the Plan.

3. **Permitted Uses and Disclosures of Protected Health Information by Business Associate.**

(a) **Functions and Activities on Behalf of the Plan.** Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform the functions, activities, or services for, or on behalf of, the Plan as previously agreed to by the parties, provided that such use or disclosure would not violate the Privacy Rule if done by the Plan.

(b) **Business Associate's Operations.** Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate and to carry out the legal responsibilities of the Business Associate. Business Associate also may disclose Protected Health Information for the proper management and administration of Business Associate, provided that disclosure is either (i) Required by Law or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person agrees to notify Business Associate of any instances of which it is aware that the confidentiality of the information has been Breached.

(c) **Minimally Necessary Use of Protected Health Information.** Business Associate will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request, except that Business Associate will not be obligated to comply with this minimum-necessary limitation if neither the Business Associate nor the Plan is required to limit its use, disclosure, or request to the minimum necessary under the HIPAA Rules. Business Associate and Covered Entity acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the HITECH Act and the HIPAA Rules.

(d) **Data Aggregation**. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to the Plan as permitted by 45 C.F.R. 164.504(e)(2)(i)(B).

(e) **No Transfer of Protected Health Information Outside the United States.** Business Associate shall not transfer Protected Health Information outside the United States without the prior written consent of the Plan. In this context, a "transfer" outside the United States occurs if Business Associate's workforce members, agents, or Subcontractors physically located outside the United States are able to access, use, or disclose Protected Health Information.

(f) **Reporting Violations of Law.** Business Associate may use Protected Health Information to report violations of law to federal and state authorities consistent with 45 C.F.R. 164.502(j)(1).

4. **Breaches and Security Incidents.**

(a) **Reporting.**

(i) *Impermissible Use or Disclosure*. Business Associate agrees to report to the Plan any use or disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware and/or any Security Incident of which it becomes aware, and to mitigate, to the extent practicable, any harmful effects of such use or disclosure that are known to Business Associate. Such notice shall be made promptly, but not later than sixty (60) days after Discovery, and thereafter upon request of the Plan.

(ii) *Notice of Breach to the Plan*. In addition to its obligations under 45 C.F.R. Part 164, Subpart D, subject to any conditions requiring a delay of a notice under 45 C.F.R. 164.412, Business Associate shall notify the Plan in writing of the Discovery of any Breach of Unsecured PHI. Such notice shall be made promptly, but not later than sixty (60) business days after Discovery, and thereafter upon request of the Plan. Such notice shall include (1) such information then-known or then-available to Business Associate that Covered Entity would be required to include in a notification to an individual under 45 C.F.R. 164.404(c), including, without limitation, the date of Discovery of such Breach, and (2) such information to allow the Plan to determine whether Business Associate constitutes Covered Entity's agent (determined in accordance with the federal common law of agency) with respect to such Breach. Business Associate will comply with all of its notification requirements under 45 C.F.R. Part 164, Subpart D within sixty (60) business days after notice from Covered Entity of its determination that Business Associate constituted its agent with respect to such Breach.

(iii) *Notice of Breach to Affected Individual(s) and Media*. Business Associate agrees to comply with the notification obligations of the Plan to affected individuals, the Secretary, and, if applicable, the media in accordance with 45 C.F.R. 164.404, 164.408, and 164.406, respectively, of any Breach by Business Associate of Unsecured PHI. Business Associate shall be responsible for any and all notification expenses arising out of its Breach to the extent that the Breach was a result of Business Associate's failure to maintain appropriate safeguards as required by this Agreement.

(b) **Mitigation of Harmful Effects.** Business Associate agrees to immediately mitigate, to the extent practicable, any harmful effect that is known to Business Associate of (i) a use or disclosure of Protected Health Information by Business Associate in violation of this Agreement, or (ii) a Security Incident with respect to E-PHI while in the possession or control of Business Associate.

5. **Obligations of the Plan Regarding Protected Health Information.**

(a) The Plan shall provide Business Associate with a copy of the Plan's notice of privacy practices as well as any changes to such notice.

(b) The Plan shall provide Business Associate with any changes in, or revocation of, authorization by an Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

(c) The Plan shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that the Plan has agreed to in accordance with 45 C.F.R. 164.522.

(d) The Plan and its representatives shall be entitled, within ten (10) business days' prior written notice to Business Associate, to audit Business Associate from time to time to verify Business Associate's compliance with the terms of this Agreement. The Plan shall be entitled and enabled to inspect the records and other information relevant to Business Associate's compliance with the terms of this Agreement. The Plan shall conduct its review during the normal business hours of Business Associate, as the case may be, and to the extent feasible without unreasonably interfering with such entity's normal operations.

6. **Compliance with EDI Rule and other Aspects of Administration Simplification Regulations.**

Business Associate agrees that, on behalf of the Plan, it will perform any transaction for which a standard has been developed under the EDI Rule that Business Associate could reasonably be expected to perform in the ordinary course of its functions on behalf of the Plan.

Business Associate agrees that it will comply with all applicable EDI standards no later than the date that the EDI Rule becomes effective with regard to Business Associate. Business Associate further agrees that it will use its best efforts to comply with all applicable regulatory provisions in addition to the EDI Rule and the Privacy Rule that are promulgated pursuant to the Administrative Simplification Subtitle of HIPAA, no later than the date such provisions become effective with regard to Business Associate.

7. **Amendment.**

The parties agree to take any action necessary to amend the Agreement from time to time as is necessary for them to comply with the requirements of the Administrative Simplification Subtitle of HIPAA. The parties may agree to amend this Agreement from time to time in any other respect that they deem appropriate. This Agreement shall not be amended except by written instrument executed by the Plan and Business Associate.

8. **Term and Termination.**

(a) **Term.** This Agreement shall be effective as of the date set forth on page 1 of this Agreement, and shall terminate when the Services Agreement terminates.

(b) **Termination for Cause.** Upon the Plan's knowledge of a material breach by Business Associate, the Plan shall provide an opportunity for Business Associate to cure the breach. If Business Associate does not cure the breach within 30 days of the date that the Plan provides notice of such breach to Business Associate, the Plan shall have the right to terminate this Agreement and the Services Agreement by providing 30 days' advance written notice of such termination to Business Associate.

(c) **Effect of Termination.**

(i) Except as provided in subparagraph (ii) immediately below, upon termination of this Agreement for any reason, Business Associate shall return all Protected Health Information to the Plan. This provision shall

apply to Protected Health Information that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(ii) In the event Business Associate determines that returning the Protected Health Information is infeasible, Business Associate shall provide to the Plan notification of the conditions that make the return infeasible. Upon mutual agreement of the parties that return of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return infeasible, for so long as Business Associate maintains such Protected Health Information.

(iii) The respective rights and obligations of Business Associate under this paragraph (c) shall survive the termination of this Agreement.

9. **Indemnification.**

Business Associate shall indemnify and hold harmless the Plan from and against any and all costs, expenses, claims, demands, causes of action, damages and judgments (including reasonable attorneys' fees) that arise out of or that may be imposed upon, incurred by, or brought against the Plan as a result of a breach of this Agreement or any violation of the Administrative Simplification Subtitle of HIPAA by Business Associate.

The Plan shall indemnify and hold harmless Business Associate from and against any and all costs, expenses, claims, demands, causes of action, damages and judgments (including reasonable attorneys' fees) that arise out of or that may be imposed upon, incurred by, or brought against Business Associate as a result of a breach of this Agreement or any violation of the Administrative Simplification Subtitle of HIPAA by the Plan.

The indemnification obligations provided for in this Section will commence on the effective date of this Agreement and shall survive its termination.

10. **Notices.**

All notices, requests, consents and other communications hereunder will be in writing, will be addressed to the receiving party's address set forth below or to such other address as a party may designate by notice hereunder, and will be either (i) delivered by hand, (ii) made by facsimile transmission, (iii) sent by overnight courier, or (iv) sent by registered mail or certified mail, return receipt requested, postage prepaid.

If to the Company via mail, hand-delivery, facsimile, or courier:

Benefit Specialist
Barton County Community College
245 NE 30
Great Bend, KS 67530
(620) 786-1167

If to the Business Associate: _____

_____

_____

_____

_____

11. **Miscellaneous.**

(a) **Severability.** All parties intend this Agreement to be enforced as written. However, (i) if any portion or provision of this Agreement will to any extent be declared illegal or unenforceable by a duly authorized court having jurisdiction, then the remainder of this Agreement, or the application of such portion or provision in circumstances other than those as to which it is so declared illegal or unenforceable, will not be affected thereby, and each portion and provision of this Agreement will be valid and enforceable to the fullest extent permitted by law; and (ii) if any provision, or part thereof, is held to be unenforceable because of the duration of such provision, the Plan and the Business Associate agree that the court making such determination will have the power to reduce the duration of such provision, and/or to delete specific words and phrases, and in its reduced form such provision will then be enforceable and will be enforced.

(b) **Headings and Captions.** The headings and captions of the various subdivisions of this Agreement are for convenience of reference only and will in no way modify, or affect the meaning or construction of, any of the terms or provisions hereof.

(c) **No Waiver of Rights, Powers and Remedies.** No failure or delay by any party hereto in exercising any right, power or remedy under this Agreement, and no course of dealing between the parties hereto, will operate as a waiver of any such right, power or remedy of the party. The terms and provisions of this Agreement may be waived, or consent for the departure therefrom granted, only by written document executed by the party entitled to the benefits of such terms or provisions. No such waiver or consent will be deemed to be or will constitute a waiver or consent with respect to any other terms or provisions of this Agreement, whether or not similar. Each such waiver or consent will be effective only in the specific instance and for the purpose for which it was given, and will not constitute a continuing waiver or consent.

(d) **Regulatory References.** A reference in this Agreement to a section in the EDI Rule or the Privacy Rule means the referenced section or its successor, and for which compliance is required.

(e) **Governing Law.** This Agreement will be governed by and construed in accordance with federal laws and, to the extent applicable, the laws of the State of Kansas.

(f) **Entire Agreement.** This Agreement sets forth the entire understanding of the parties with respect to the subject matter set forth herein and supersedes all prior agreements, arrangements and communications, whether oral or written, pertaining to the subject matter hereof.

(g) **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Plan to comply with the Administrative Simplification Subtitle of HIPAA.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date specified in the opening paragraph of this Agreement.

_____
Name of Business Associate Entity

By: _____

Title: _____

Date: _____

Barton County Community College Organized Health Care Arrangement
Barton County Community College

By: _____

Title: _____

Date: _____

WHAT EMPLOYERS NEED TO KNOW
ABOUT THE
HIPAA MEDICAL PRIVACY REGULATIONS

PRESENTED BY

HINKLE
LAW FIRM LLC

WHAT EMPLOYERS NEED TO KNOW ABOUT THE HIPAA MEDICAL PRIVACY REGULATIONS

by

Hinkle Law Firm LLC
1617 North Waterfront Parkway
Suite 400
Wichita, Kansas 67206-6639
www.hinklaw.com

I. **Introduction.** Making sense out of the HIPAA medical privacy regulations is not easy. The regulations are long, they are complicated, and they use so many defined terms that they might as well be written in a foreign language. But ignoring the regulations is not an option. The regulations have the force of law, so employers (and the attorneys advising them) have no choice but to figure out what is required and then to comply as best they can.

II. **Background to the Regulations.** In making sense out of the regulations, it may be helpful to know something about their background.

A. When the Health Insurance Portability and Accountability Act of 1996 (or "HIPAA") was first enacted, it was commonly thought of as a law that made it easier for people to change jobs by limiting the application of pre-existing condition exclusions.

B. There is more to HIPAA, however, than just "portability." HIPAA also contains a number of "administrative simplification" requirements.

C. The idea behind these "administrative simplification" requirements was to reduce health care costs by standardizing the electronic processing of claims.

1. The thinking was that doctors' offices would no longer have to employ large staffs of people to code information in the various formats required by insurance companies and that insurance companies would be able to share information easily with each other because everyone would be using a standard format and a standard set of codes.

2. This led to the electronic data interchange (or "EDI") regulations. The EDI regulations require the use of standard electronic formats and standard code sets in certain standard transactions. These regulations are briefly discussed in Section XXIII of this outline.

D. Congress recognized that the use of standard formats and standard code sets could also lead to some problems. If information became easier to share, then it was likely that more information would be shared and that information that had been private before, simply by virtue of being hard to find and hard to read, could become a lot less private.

E. Congress decided to address this in two different ways.

1. First, it decided to protect electronic information from unauthorized or unintentional disclosures. This has been addressed by the final "security" regulations that were issued by the Department of Health and Human Services ("HHS") in February 2003. 68 Fed. Reg. 8333 (Feb. 20, 2003).

2. Of course, you can't protect information from unauthorized disclosure unless you know who is authorized to receive it and who is not. So Congress also decided to protect the information itself by limiting who is allowed to access health information and what they are allowed to use it for and by giving people a right to see their own information, to request changes to their information, and to request an accounting of disclosures that have been made of their information.

F. Congress could not agree on what uses of medical information should, or should not, be allowed, so Congress enacted HIPAA without deciding the issue. Instead, it set a deadline for itself to act by passing a medical privacy law. It further provided that, if it failed to act by August 1999, the HHS would be required to issue medical privacy regulations. HIPAA § 264(c) (Public Law 104-191, August 21, 1996).

G. Congress failed to act by the August 1999 deadline, so HHS moved forward with the medical privacy regulations. These were published in final form in December 2000 and were modified in August 2002. 65 Fed. Reg. 82462 - 82829 (Dec. 28, 2000); 67 Fed. Reg. 53182 - 53273 (Aug. 14, 2002).

H. In 2008, Congress enacted the Genetic Information Nondiscrimination Act ("GINA"), which, in part, prohibited the use or disclosure of genetic information for underwriting purposes. (Public Law 110-233, May 21, 2008.) The provisions of GINA affecting HIPAA medical privacy rules became effective for plan years beginning after May 21, 2009.

I. In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which was passed as part of the American Recovery and Reinvestment Act of 2009. Among other things, HITECH extended certain privacy and security obligations directly to business associates, enacted new notification requirements upon a "breach" of unsecured protected health information, and provided for stricter penalties for violations. (Public Law 111-5, February 17, 2009.) HHS adopted interim final regulations to implement the HITECH Act amendments. 74Fed. Reg. 42740 (Aug. 24, 2009) and 74 Fed. Reg. 56123 (Oct. 30, 2009).

J. In January 2013, HHS replaced the interim final "breach" regulations with final regulations that made significant changes to the requirements for breach notifications. These are referred to throughout this outline as the "2013 final regulations." 78 Fed. Reg. 5566 (Jan. 25, 2013).

III. **Application of the Regulations to Employers.** The regulations do not apply directly to employers. They do, however, apply to "covered entities." This includes most healthcare providers, healthcare clearinghouses, and – significantly for us – most employer-sponsored group health plans. 45 CFR § 160.102(a). Thus, the regulations affect employers in an indirect way.

IV. **What is a "Health Plan"?** One of the things that most people seem to struggle with is the idea or definition of a "health plan."

A. If you ask a typical employee or even a typical business owner to give you the name of their health plan, they will probably give you the name of an insurance company.

1. For example, if you ask one of the employees of our firm what our health plan is, they'll probably tell you "Blue Cross."

2. What you will not hear – outside of the Employee Benefits Group, of course – is the "Hinkle Law Firm LLC Employee Group Medical Plan" because that is not how we think of things.

B. From an employee benefits perspective, however, that's where family coverage is coming from. And that's what the drafters of the regulations were thinking of when they used the term "health plan."

V. **ERISA "Employee Benefit Plans."** To understand the relationship between an employer and an employer-sponsored health plan, it helps to know something about the Employee Retirement Income Security Act of 1974 (or "ERISA").[1]

A. ERISA applies to "employee benefit plans" offered by businesses to their employees. Under ERISA, there are two types of "employee benefit plans":

1. Employee pension benefit plans; and

2. Employee welfare benefit plans.

ERISA § 3(3).

B. An "employee pension benefit plan" is basically a plan that provides retirement income or that defers income beyond the end of the employee's period of covered employment. ERISA § 3(2). That's reasonably easy to understand and most people have an intuitive grasp of what is, or is not, a "pension benefit plan."

[1]ERISA is codified at 29 U.S.C. §§ 1001 et seq.; however, ERISA sections are commonly cited according to the section number in Public Law No. 93-406, and not as they appear in the United States Code. We will follow that convention in this outline.

C. Understanding what is or is not an "employee welfare benefit plan" is a little harder for most people. ERISA defines an "employee welfare benefit plan" as:

1. "Any plan, fund, or program"

2. that is "established or maintained by an employer"

3. for the purpose of providing for its participants and their beneficiaries any of the following benefits (among others):

   a. Medical, surgical, or hospital care;

   b. Benefits in the event of sickness, accident, disability, death, or unemployment; or

   c. Severance benefits.

4. whether those benefits are provided through the purchase of insurance or otherwise.

ERISA § 3(1).

If an employer is providing these types of benefits to it employees – and the employer is not a church or a governmental entity – an ERISA "welfare benefit plan" probably exists. It doesn't matter how the coverage is paid for. It doesn't matter if it is employer paid, employee paid, or both. It is probably an ERISA plan.[2] *See, e.g., Peckham v. Gem State Mut. of Utah*, 964 F.2d 1043, 1048-49 (10th Cir. 1992) (holding that an employer had established a "plan, fund, or program" by making medical coverage available to its employees).

D. Common examples of ERISA welfare benefit plans include medical plans, dental plans, group life plans, health flexible spending accounts, and (to the surprise of many) employee assistance programs (or "EAPs").

[2] We say "probably" because there are a few exceptions. Although the language of ERISA itself is broad, the Department of Labor has the authority to issue clarifying regulations. Pursuant to this authority, the DOL has recognized an exception for certain "payroll practices," such as the payment of wages, "unfunded" sick pay, and "unfunded" time off from work. DOL Regs. § 2510.3-1(b). The DOL has also recognized an exception for certain insurance products offered through the workplace where the employees pay the entire cost and the role of the employer is essentially limited to deducting the cost from the employees' paychecks. DOL Regs. § 2510.3-1(j). Arrangements falling within this exception are commonly referred to as "voluntary employee-pay-all arrangements." Employers should be cautious about relying on this exception as it can be difficult to fit within and the applicability of this exception has been litigated in numerous cases, typically after an employee has filed suit challenging an insurance company's decision to deny benefits.

VI. **ERISA Requirements.** ERISA has a number of different requirements. One of these requirements is that the plan must be established and maintained according to the terms of a written plan document. ERISA § 402.

A. The plan document is supposed to contain all of the rules under which the benefit is being provided.

B. The intent is to promote the consistent administration of the plan and to prevent *ad hoc* decision making.

C. The problem is that a lot of employers do not have a plan document.

D. A contract of insurance, by itself, is not normally enough to satisfy the plan document requirement. A normal contract of insurance simply does not contain all of the terms and provisions that are required by ERISA.

E. The plan document requirement is important because (among other reasons), subject to some exceptions, the medical privacy regulations require employers to add various provisions to their plan document if the employer will have access to "protected health information" (or "PHI").

F. If an employer is under the impression that its plan document is the same as its insurance contract, this particular requirement in the privacy regulations is bound to be confusing.

VII. **What is "Protected Health Information"?** The regulations limit the use and disclosure of "protected health information" by "covered entities." Consequently, understanding what is, or is not, PHI is important.

A. *"Health Information."* To understand the definition of PHI, it is helpful to begin with the definition of "health information." "Health information" is defined as information:

1. That is *created or received* by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; *and*

2. That relates to:

   a. the past, present, or future physical or mental health or condition of an individual; or

   b. the provision of health care to an individual; or

   c. the past, present, or future payment for the provision of health care to an individual.

45 C.F.R. § 160.103. This is obviously a broad definition. It takes in almost any information about a person's health that an employer might learn.

B. *"Individually Identifiable Health Information."* The next step in understanding the definition of "protected health information" is to look at the definition of "individually identifiable health information." For "health information" to constitute "individually identifiable health information," it must:

1. Be *created or received* by a health care provider, health plan, employer, or health care clearinghouse; *and*

2. Either identify the individual or provide a reasonable basis for believing that the information could be used to identify the individual.

45 C.F.R. § 160.103. The definition of "individually identifiable health information" is narrower than the definition of "health information" in two respects: (1) First, it does not include information that is created or received by a public health authority, life insurer, or a school or university; and (2) second, it adds the requirement that the information must identify, or provide a basis for identifying, the individual to whom the information relates.

C. *"Protected Health Information."* "Protected health information," (or "PHI") is essentially defined as "individually identifiable health information" that is "maintained or transmitted" in any form or medium and for which no exception applies. The regulations list the following exceptions:

1. Employment records held by a "covered entity" in its role as an employer. The preamble to the regulations states that this exclusion was added to make it clear that information held by a "covered entity" does not automatically become PHI merely because it relates to an employee's health.[3]

2. Education records covered by the Family Educational Rights and Privacy Act.

3. Records on a student 18 or older made by a healthcare professional for the purpose of treating the student. 45 C.F.R. § 160.103.

VIII. **How Do the Regulations Affect an Employer that is Sponsoring a Group Health Plan?** The answer to this question depends on two things:

A. First, is the plan "fully-insured" or "self-insured" (also known as "self-funded")?

B. Second, how much PHI does the employer receive (or need to receive) from the plan?

[3] Note that this exception does not apply to employment records held by any and all employers. The exception applies only to employment records held by a "covered entity" in its role as an employer. Thus, for example, if a machine shop holds information about the health of an employee, that information will technically constitute PHI whereas the same information held by a medical office regarding one of its employees will not constitute PHI due to this exception. For reasons explained later in this outline, however, the practical significance of this distinction is limited.

The effect that the answers to these two questions have is summarized on the following chart:

Type of Plan	***Level of Employer Involvement with PHI***	***Privacy Requirements that Apply to the Employer and to the Plan***	***PHI that may be Disclosed by the Plan (or Insurance Company) to the Employer***
Fully-Insured	"Hands-off PHI" (i.e., no access to PHI), other than limited access to "summary health information" for the purpose of obtaining bids for coverage and/or modifying, amending, or terminating the plan.	None (except Employer [1] cannot require individuals to waive their HIPAA rights and [2] cannot engage in retaliation against, or attempt to intimidate, individuals who are exercising their HIPAA rights, such as filing a complaint or opposing an improper practice).	None, although the employer may have access to a limited amount of "summary health information" for purposes of obtaining bids for coverage and/or modifying, amending, or terminating the plan. The employer may also have access to enrollment and disenrollment information provided by the insurance company.
Fully-Insured	PHI shared with employer for "plan administration functions."	(1) Employer must amend plan document to include provision authorizing limited disclosure of PHI to the employer; (2) Employer must implement a "firewall" to limit the use or disclosure of PHI to those persons who are authorized in the plan document to have access to PHI; (3) Plan must prepare a privacy notice for plan participants; (4) Plan is subject to "administrative safeguards," including requirements to (a) develop and implement written privacy procedures, (b) designate a privacy officer, (c) train employees, (d) establish a process by which participants may make complaints, and (e) develop a system of sanctions for those employees who violate the plan's procedures.	As described in the plan document, but limited to the "minimum necessary."
Self-Insured	PHI shared with employer for "plan administration functions."	Generally the same as above, although, there may be some differences in the application of particular requirements. For example, a self-insured plan must provide a privacy notice to all participants whereas a fully-insured plan is only required to provide the notice upon request.	Same as above.
Self-Insured and Self-Administered with fewer than 50 participants	Administered by the Employer (as opposed to being administered by a "third party administrator").	None (because the plan is not a covered entity).	No restrictions (because the plan is not a covered entity and the medical privacy regulations do not, for that reason, apply).

IX. **Overview of Requirements Applicable to Covered Entities.** The requirements that apply to covered entities under the regulations fall into three broad categories:

A. *Use or Disclosure of PHI.* First, the regulations prohibit a covered entity from using or disclosing PHI except as permitted by the regulations. This requirement is discussed in more detail in Section X of this outline.

B. *Individual Rights.* Second, subject to certain exceptions, the regulations give individuals various rights with respect to their own PHI. These rights include the following rights:

1. To inspect and copy their PHI. 45 C.F.R. § 164.524(a)(1);

2. To request amendments or corrections to PHI if they believe that it is inaccurate or incomplete. 45 C.F.R. § 164.526(a);

3. To obtain an accounting of the disclosures that have been made of their PHI (subject to various exceptions, including disclosures that have been made for treatment, payment, or health care operations). 45 C.F.R. § 164.528(a);

4. To receive a notice of privacy practices from a covered entity describing the following:

   a. The uses or disclosures of PHI that may be made by the covered entity;

   b. The individual's rights; and

   c. The covered entity's legal duties with respect to the PHI;

   45 C.F.R. § 164.520(a).

5. To request additional restrictions on the use or disclosure of their PHI (although the covered entity is not required to agree to this request, (except in the limited cases of self-payment by the individual)). 45 C.F.R. § 164.522(a); and

6. To request that PHI be communicated to the individual by alternative means or at alternative locations. Health care providers must accommodate such requests if they are "reasonable." Health plans must accommodate such requests if they are "reasonable" and if the individual "clearly states that the disclosure of all or part of that information could endanger the individual." 45 C.F.R. § 164.522(b).

C. *Administrative Safeguards.* Third, the regulations require covered entities to protect PHI against unauthorized use or disclosure. To accomplish this, a covered entity must do the following (among other things that are not listed):

1. Designate a "privacy officer" who will be responsible for developing and implementing privacy policies and procedures. 45 C.F.R. § 164.530(a)(1)(i);

2. Designate a contact person or office to which complaints can be made. 45 C.F.R. § 164.530(a)(1)(ii);

3. Provide training to its "workforce" regarding privacy policies and procedures. 45 C.F.R. § 164.530(b);

4. Establish appropriate safeguards against the unauthorized use or disclosure of PHI, including:

   a. Administrative safeguards – for example, establishing and enforcing policies and procedures;

   b. Technical safeguards – for example, taking steps to limit access to PHI on computer systems and networks; and

   c. Physical safeguards – for example, keeping PHI in locked file cabinets.

   45 C.F.R. § 164.530(c).

X. **Use or Disclosure of PHI.**

A. *General Rule.* A covered entity may not use or disclose PHI *except* as permitted by the regulations. 45 C.F.R. § 164.502(a). Under the regulations, PHI may be used or disclosed in the following circumstances:

1. To an individual in accordance with that individual's right to access his/her own PHI. 45 C.F.R. § 164.502(a)(1)(i);

2. For "covered functions," that is, for treatment, payment, or healthcare operations. 45 C.F.R. § 164.502(a)(1)(ii);

3. After the individual has had the opportunity to object or agree, but only as to:

   a. "Directory information," such as whether an individual is a patient at a hospital, where the patient is located, and what the patient's general condition is; or

b. Disclosures made to a limited category of persons, such as family members and close friends if the information disclosed is "directly relevant to such person's involvement with the individual's care or payment related to the individual's care";

45 C.F.R. § 164.502(a)(i)(v).

4. Pursuant to an individual's authorization. 45 C.F.R. § 164.502(a)(1)(iv); and

5. As required or permitted under HIPAA's public policy exceptions, including (among other things not listed):

a. Disclosures for worker's compensation;

b. Disclosures for law enforcement purposes;

c. Disclosures for judicial and administrative proceedings; and

d. Disclosures required by HHS in connection with its enforcement and compliance review actions.

45 C.F.R. § 164.502(a)(1)(vi).

B. *"Minimum Necessary" Rule.* As a general proposition, most disclosures are subject to the "minimum necessary" standard. In other words, a covered entity must limit the amount of PHI that it uses, requests, or discloses to the minimum amount necessary for the purpose identified by the requesting party. The "minimum necessary" rule does not apply to requests submitted by or disclosures made to a health care provider in connection with treatment that is being provided to the individual. 45 C.F.R. § 164.502(b).

XI. **Employers and Other Entities That Are Not Covered Entities.** When Congress authorized HHS to draft medical privacy regulations, it left a rather large hole: HHS was given the authority to regulate covered entities – that is, to regulate health care providers, health care clearinghouses, and group health plans – but, even though many other people routinely have access to PHI in the healthcare system, HHS was not given the authority to regulate anyone else.

HHS "solved" this problem in a rather creative way: If it could not control the conduct of these other people directly, it would do so indirectly by regulating the ways in which "covered entities" could interact with these other people.

Thus, the regulations prohibit "group health plans" from sharing PHI with the employer-plan sponsor (in most situations) unless the employer has agreed to limit its use of the PHI through amendments to the plan document and through a certification given to the plan. Similarly, the regulations prohibit group health plans and other

covered entities from sharing PHI with business associates unless there is a written contract containing specified provisions limiting the use of the PHI by the business associate. These rules are explained in more detail below.

Recently, as part of the HITECH Act, Congress extended many HIPAA privacy and security mandates to apply directly to business associates. Covered entities will still need written agreements with their business associates, but now, business associates will be directly liable under federal law if they violate the applicable privacy and security rules.

XII. **Sharing PHI with the Employer-Plan Sponsor.**

A. *General Rule.* As a general rule, an employer-sponsored group health plan may not share PHI with the employer except in the following circumstances:

1. "De-identified information" may be shared because the removal of identifying information causes the information to fall outside the definition of PHI. 45 C.F.R. § 164.502(d);

2. "Summary health information" may be shared for the limited purpose of obtaining premium bids for insurance coverage and/or considering plan amendments or plan termination. 45 C.F.R. § 164.504(f)(1)(ii). "Summary health information" is essentially the same as "de-identified information" except that "summary health information" may include a five digit ZIP code for each participant. 45 C.F.R. § 164.504(a);

3. Information as to whether an individual is enrolled or has disenrolled in an employer-sponsored group health plan may be shared with the employer. 45 C.F.R. § 164.504(f)(iii);

4. PHI may be shared if an individual signs an "authorization." Authorizations are discussed in Section XVIII of this outline; and

5. PHI may be shared with the sponsoring employer for "plan administration functions" <u>if</u> the employer amends the plan documents to limit the ways in which the PHI may be used and the persons to which it may be disclosed. 45 C.F.R. § 164.504(f)(1)(i). Plan administration functions include such things as quality assurance, claims processing, auditing, and monitoring. Plan administration functions do <u>not</u>, however, include employment-related functions or functions in connection with other benefits. 45 C.F.R. § 164.504(a); 65 Fed. Reg. at 82508.

B. *Plan Document Amendments.* In order to receive PHI for "plan administration functions," an employer must amend its plan document. The amendments must:

1. Establish "the permitted and required uses and disclosures" of PHI by the employer;

2. Prohibit the employer from using or further disclosing the PHI "other than as permitted under the plan document or as required by law";

3. Require the employer to ensure that agents or subcontractors to which it provides PHI agree to the same restrictions and conditions that apply to the employer itself with respect to the PHI;

4. Prohibit the employer from using or disclosing the PHI for employment-related actions or in connection with any other employee benefit plan;

5. Require the employer to report to the group health plan any use or disclosure of the PHI that is inconsistent with the permitted uses or disclosures, including reporting any breach of unsecured PHI that it discovers (as required by the 2013 final regulations);

6. Restrict the disclosure of PHI of an individual (unless the disclosure is otherwise required by law) where the disclosure is to the group health plan for purposes of carrying out payment or health care operations (and not treatment) and the PHI pertains to a health care item or service for which the health care provider has been paid out-of-pocket in full;

7. Require the employer to make PHI available to plan participants, consider their requested amendments to their PHI, and, upon their request, provide them with an accounting of the employer's PHI disclosures;

8. Require the employer to make its internal practices and records relating to the use and disclosure of PHI received from the group health plan available to HHS upon request;

9. Require the employer, if feasible, to return or destroy all PHI received from the group health plan if that information is no longer needed for the purpose for which disclosure was made or, if that is not feasible, to limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the PHI infeasible;

10. Ensure that there is "adequate separation" – or, as it is sometimes referred to, a "firewall"– between the group health plan and the employer by:

    a. Describing the employees, class of employees, or other persons under the control of the employer who may be given access to PHI;

    b. Restricting access to and use of PHI by such persons to the "plan administration functions" that the employer performs for the group health plan; and

c. Providing an "effective mechanism" for resolving "any issues of non-compliance" with the provisions of the plan document by persons having access to the PHI.

11. Prohibit the plan from sharing PHI with the employer unless the employer certifies to the plan that the provisions listed above have been adopted and that the employer agrees to comply with those provisions; and

12. Require that, if the employer creates, receives, maintains, or transmits any electronic PHI (other than enrollment and disenrollment information and summary health information, which are not subject to these restrictions) on behalf of the group health plan, it will do the following:

a. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI;

b. Ensure that any agent (including subcontractors) to whom it provides such electronic PHI agree to implement reasonable and appropriate security measures to protect the information; and

c. Report to the group health plan any security incident of which it becomes aware.

45 C.F.R. § 164.504(f)(2).

XIII. **Reasons Employers Might Need PHI from a Group Health Plan.** There are two principal reasons why an employer and/or its broker might need (or want) to have access to PHI from the insurance carrier (or claims administrator) for the employer's group health plan.

A. *To Ensure that Claims Are Being Correctly Processed.* The first reason is to make sure that the insurance company is correctly processing claims. Particularly with large claims, it is common for an employer and/or its broker to make sure that the claim is properly payable by the plan. Situations in which a claim might not be payable by the plan include the following:

1. *Coordination of Benefits.* The claim should have been paid by someone other than the group health plan. For example, the claim should have been paid under the spouse's plan, through the worker's compensation system, or through the "personal injury protection" benefits under an automobile liability policy.

2. *Person is Not Covered Under the Plan.* The claim is for a person who is not covered under the plan. For example, it may be that the person is no longer part of the group. This could include a person who is no longer employed by the employer and who did not elect COBRA. It could also include a divorced spouse who is still being covered as a dependent (rather than as

a COBRA beneficiary) because the employee failed to inform the group health plan of the divorce. Or, it could be a situation in which the person was never part of the group but the claim was posted to the group by mistake.

3. *Benefits are Not Payable Under the Plan.* The benefit sought is not a benefit that is provided by the plan. Although one would generally expect an insurance company to know what benefits are payable and what are not, mistakes do sometimes happen. If the employer does not receive detailed information about the claims that have been paid, it is possible that a mistake of this type would never be caught.

B. *To Obtain Bids from Other Insurance Companies.* The second reason an employer and/or its broker might need (or want) PHI is to obtain bids from other insurance companies when coverage is up for renewal. As a general proposition, rates are based on the actual claims experience of a group. This actual claims experience would be reflected in the "summary health information" for the group, but there may be times when further analysis is warranted. Such situations include the following:

1. *Confirming the Accuracy of the Summary Health Information.* It is possible that the group's summary health information contains mistakes. As noted above, for example, the summary health information might reflect claims that were not properly payable under the plan, such as claims that should have been paid by worker's compensation, claims for persons not covered under the plan, or claims for benefits that were not payable under the plan. Again, if the employer does not know the name of the person incurring the claim, it is doubtful that this type of mistake could be caught.

2. *Identifying Non-Recurring Claims.* If a group has incurred large claims in the recent past, the rate that is quoted is likely to be higher than for a comparable group that has not had such claims. If, however, an employer or broker is able to persuade an insurance carrier that the group is healthier than its prior claims experience might indicate, a more favorable rate should be quoted. This could be the case, for example, if a person who incurred a large claim is no longer part of the group. This could be because the person has died or because the covered participant left the group without electing COBRA. Without knowing the names of the persons who have incurred large claims, however, an employer or broker may have a difficult time identifying such claims and calling them to the attention of the prospective carrier.

C. *What the Regulations Allow.* An employer-plan sponsor may obtain PHI from its group health plan if that information is needed for plan administration functions that are being performed by the employer on behalf of the plan.

1. Ensuring that the claims are being paid when they are properly payable under the terms of the plan and that they are being denied when they are not properly payable would appear to be a type of plan administration function. Consequently, it appears that an employer may obtain PHI for this purpose, assuming, of course, that the conditions for receiving this information (such as the adoption of plan amendments and the implementation of a firewall) have been satisfied.

2. Obtaining coverage for the plan, on the other hand, may or may not be considered to be a plan administration function under the regulations. Consequently, it is not clear whether the regulations will allow an employer to obtain PHI for this purpose.

    a. If PHI is needed for underwriting purposes, the plan is allowed to share that PHI with its business associates pursuant to a business associate agreement. Thus, the plan would be allowed to share PHI with an insurance broker, assuming a valid business associate agreement is in place.

    b. But the plan is *not* allowed to share PHI with the employer-plan sponsor for underwriting purposes (as opposed to being shared for "plan administration" functions). Under the regulations, it appears that the information that may be shared with the employer for underwriting purposes is limited to summary health information only.

XIV. **The Security Rule and Electronic PHI.**

A. *General Rule.* The electronic security regulations are essentially intended to prevent unauthorized persons from gaining access to PHI that is stored or transmitted electronically. Of particular concern are laptops, home-based computers, smartphones, USB flash drives, email, public workstations, and public wireless access. Some of the security rules are very similar to the privacy rules (e.g., sanctions, training, documentation, policies and procedures, business associate contracts, etc.). Other rules dovetail so that steps that have been taken for privacy compliance can form the basis for security compliance.

B. *Application to Employers.* The electronic security regulations take the same approach to employers as the privacy regulations. That is, the rules apply directly to group health plans, but they do not apply directly to employers. Employers, however, must agree to do what the regulations require as a condition of accessing PHI in electronic form from their group health plans. (Note: after February 18, 2010, most of the provisions of the security rule also apply directly to *business associates*.)

C. *Standards and Implementation Specifications.* The security rule requires the establishment of certain administrative, physical, and technical safeguards (called "standards and implementation specifications"), for PHI that is transmitted by, or

maintained in, electronic media. 45 CFR §§ 164.308, 160.310, and 160.312. The security rule, however, allows great flexibility in determining how to comply with the rule's requirements. An entity may use any security measures that allow it to reasonably and appropriately comply with the standards and implementation specifications contained in the rule. In deciding which security measures to use, an entity must perform a risk analysis.

D. *Purpose of Safeguards.* There are four main goals of implementing the administrative, physical, and technical safeguards that are required by the security regulations:

1. Ensure the confidentiality, integrity, and availability of electronic PHI;

2. Protect against reasonably anticipated threats or hazards to the security or integrity of the electronic PHI;

3. Protect against reasonably anticipated unauthorized uses or disclosures of the electronic PHI; and

4. Otherwise ensure that officers and employees of the entity comply with the security rule.

SSA § 1173(d)(2); 45 CFR § 164.306(a).

E. *Compliance with the Standards and Implementation Specifications for Group Health Plans*. The compliance burden on group health plans is limited compared to other covered entities. Group health plans are essentially pieces of paper, i.e., plan documents. As such, they have no workforce, no hardware, no software, no premises, no facilities, and no electronic information systems. The holders of plan PHI are business associates, insurers, and the employer that sponsors the group health plan. As a result, the group health plan's obligations under the security rule may be limited to those standards and implementation specifications that do not address workforce, hardware software, premises, facilities, or information systems. This basically leaves the following obligations for group health plans:

1. Appointment of a security officer;

2. Performance of a risk analysis (which would determine that all electronic PHI is in the hands of business associates or the employer/plan sponsor);

3. Development of risk management procedures (which would be limited because all electronic PHI is in the hands of business associates or the employer/plan sponsor);

4. Periodic evaluation to determine whether anything has changed that would require a change in the risk analysis or risk management procedures; and

5. Ensuring that business associate contracts or a plan amendment (or both) are in place and comply with the security requirements.

XV. **Breach Notifications Under the 2013 Final Regulations.**

A. *What is a Breach?* A "breach" is the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such PHI. 45 CFR § 164.402. The following three types of unauthorized acquisition, access, use, or disclosure are excluded from the definition of a "breach:"

1. Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the group health plan if such acquisition, access, or use was made in good faith and within the course and scope of employment or other professional relationship of such employee or individual, respectively, with the group health plan, and the information is not further acquired, accessed, used, or disclosed by any person in a manner not permitted by the medical privacy or security rules;

2. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by the group health plan to another similarly situated individual at the same facility so long as the information received is not further used or disclosed in a manner not permitted by the medical privacy or security rules; and

3. Any disclosure to an unauthorized person where the PHI that was disclosed would not reasonably have been retained by such person.

B. *What is Unsecured PHI?* Breaches are only reportable if they involve "unsecured" PHI. Unsecured PHI means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HHS. 45 CFR § 164.402. Only two methods are identified for rendering PHI unusable, unreadable, or indecipherable – encryption and destruction.

C. *Performance of a Risk Assessment to Determine if PHI Has Been "Compromised."* Group health plans (and business associates) must perform a four-factor risk assessment to determine if PHI has been compromised. After all, an unauthorized use or disclosure could occur, but if the PHI is not actually "compromised," a breach will not exist. The four-factor risk assessment should take into account the following:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

45 CFR § 164.402.

D. *Breach Notification for Group Health Plans.* If, after performing a risk assessment, a group health plan determines that a breach of unsecured PHI has occurred, the plan must notify the affected individuals, HHS, and, in certain instances, the media, as follows:

1. *Notification to Individuals.* Individuals must be notified of the breach without unreasonable delay and in no case later than 60 calendar days after the breach is discovered (or should have been discovered through exercising reasonable diligence). The regulations are specific regarding information that must be included in the notification.

2. *Notification of HHS.* The timing of the notification to HHS and the type of notification depend on whether or not the breach involved 500 or more individuals, as follows:

a. *Breaches Involving 500 or More Individuals.* If a breach of unsecured PHI involves 500 or more individuals, a group health plan must notify the Secretary of HHS at the same time the individual notice is given. The manner for notifying the Secretary is set forth on the HHS website.

b. *Breaches Involving Less than 500 Individuals.* If a breach of unsecured PHI involves less than 500 individuals, a group health plan must maintain a log or other documentation of the breaches and notify the Secretary of HHS of these breaches within 60 days after the end of the calendar year in which the breaches were discovered. The group health plan will consult the HHS website for instructions for submitting the notification.

3. *Notification to the Media.* The media need only be notified if the breach of unsecured PHI involves more than 500 residents of a State or jurisdiction. If more than 500 residents of a State or jurisdiction are involved, a group health plan must notify prominent media outlets serving that State or jurisdiction of the breach. This notification must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.

E. *Breach Notification for Business Associates.* A business associate must provide notice of a breach to a covered entity without unreasonable delay and in no case later than 60 calendar days following the discovery of the breach. 45 CFR § 164.410(b).

XVI. **Business Associates.** A "business associate" is a person or entity that (1) performs a function or activity on behalf of a covered entity or provides certain specific services for a covered entity; and (2) has access to PHI. In addition, in a significant change brought about by HITECH and the 2013 final regulations, *subcontractors* (and subcontractors of subcontractors) are now "business associates" if they create, receive, maintain, or transmit PHI on behalf of a business associate. 45 C.F.R. § 160.103.

A. Examples of a business associate could include the following:

1. The plan's auditors and accountants, particularly if the auditor examines individual claims;

2. The plan's actuaries, particularly if the actuary reviews potential large claims, reviews reinsurance reimbursements, or has access in some other way to information about individual claims;

3. The plan's attorneys if the attorneys review or provide advice with respect to individual claims;

4. Consultants who provide advice to the plan, if the consultant has access to information about individual claims; and

5. Claims administrators and third party administrators.

B. The term "business associate" does not, however, include the following:

1. Members of the covered entity's workforce, including employees, volunteers, trainees, and other persons who are under the direct control of the covered entity;

2. A plan sponsor, with respect to disclosures by a group health plan to the sponsor, to the extent the sponsor has complied with the requirements to receive PHI from the plan; and

3. Financial institutions, if (to oversimplify somewhat) the involvement of the financial institution is limited to the processing, clearing, or settling of checks or other financial instruments. For example, if a check is drawn on a bank in order to pay a claim to an individual participant, the bank does not thereby become a business associate of the plan.

45 C.F.R. § 160.103.

C. Business associates (including subcontractors) are directly liable for many violations to HIPAA privacy and security provisions, including the following:

1. Impermissible uses and disclosures of PHI;

2. Failure to provide breach notifications to the covered entity;

3. Failure to provide access to a copy of electronic PHI to the covered entity, the individual, or the individual's designee;

4. Failure to provide an accounting of disclosures; and

5. Failure to comply with the requirements of the security rule.

[Pub. L. No. 111-5 (2009), § 13401; 78 Fed. Reg. 5565, 5589, 5597-99 (Jan. 25, 2013).]

Note that, prior to changes made by the HITECH Act and the 2013 final regulations, business associates were only indirectly subject to the HIPAA rules. Civil penalties that apply to business associates who violate HIPAA security provisions and many of HIPAA's privacy provisions are discussed in Section XXI.

XVII. **Doing Business with a Business Associate.**

A. *General Rule.* The regulations provide that a covered entity may disclose PHI to a business associate and may allow the business associate to create, receive, maintain, or transmit PHI on its behalf only if the covered entity receives "satisfactory assurance" that the business associate will adequately safeguard the information. This is done by entering into a "business associate contract" (also referred to as a "business associate agreement"). (Note: A covered entity is not required to obtain such "satisfactory assurance" from a business associate that is a subcontractor.) 45 C.F.R. § 164.502(e). The business associate contract must:

1. Establish the permitted and required uses and disclosures by the business associate, which may not exceed the uses and disclosures that are allowed for the covered entity. 45 C.F.R. § 164.504(e)(2)(i);

2. Prohibit the business associate from using or disclosing the information other than as permitted by law. 45 C.F.R. § 164.504(e)(2)(ii)(A);

3. Require the business associate to implement safeguards to prevent the improper use and disclosure of electronic PHI. 45 C.F.R. § 164.504(e)(2)(ii)(B);

4. Require the business associate to report to the covered entity when it becomes aware of any uses or disclosures of information not provided for by the business associate contract, including breaches of unsecured PHI, as required by the breach notification rules. 45 C.F.R. § 164.504(e)(2)(ii)(C);

5. Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such PHI. 45 C.F.R. § 164.504(e)(2)(ii)(D);

6. Require the business associate to make PHI available to an individual consistent with the individual's right to access, amend, and receive an accounting related to such information. To the extent that the business associate is to carry out these obligations directly under the agreement, require the business associate to comply with the privacy rule requirements that apply to the covered entity with respect to these rights. 45 C.F.R. § 164.504(e)(2)(ii)(E)-(H);

7. Require the business associate to make its internal practices, books, and records available to HHS for purposes of determining the covered entity's compliance with HIPAA. 45 C.F.R. § 164.504(e)(2)(i)(I);

8. Require the business associate to return or destroy all PHI associated with the covered entity upon termination of the business associate contract, if such is feasible, or to continue to protect the PHI, by extending the protections of the business associate contract and limiting further uses and disclosures to those purposes that make the return or destruction of the information infeasible. 45 C.F.R. § 164.504(e)(2)(i)(I); and

9. Authorize the covered entity to terminate the business associate contract if the business associate has violated a material term of the contract. 45 C.F.R. § 164.504(e)(2)(iii).

B. *Responsibility for Compliance on the Part of a Business Associate.* When a covered entity discovers non-compliance on the part of a business associate, the covered entity (or business associate, when dealing with subcontractors) is required to take reasonable steps to cure the breach or end the business associate contract if it becomes aware of a material violation. Willful ignorance of the business associate's activities is not a defense. 45 C.F.R. §§ 164.314(a)(1)(ii) and 164.504(e)(1). Covered entities and business associates are liable for violations committed by their agents (including a workforce member) acting within the scope of the agent's authority. The analysis of whether a business associate is an agent will be fact specific, taking into account the terms of a business associate contract as well as the totality of the circumstances involved in the ongoing relationship between the parties. 45 CFR § 160.402(c).

C. *Deadline for Amending Business Associate Contracts.* The 2013 final breach regulations require business associate contracts that were already in place to be amended. The deadlines for adding required provisions into existing contracts are summarized in the chart at the end of this outline.

XVIII. **Authorizations.** A covered entity may disclose PHI to virtually anyone if the individual gives his/her permission by signing an "authorization." An authorization must be in writing and must contain six "core elements" as well as certain other statements. 45 C.F.R. § 164.508.

A. *Core Elements.* The core elements that must be present in all authorizations are as follows:

1. A "specific and meaningful" description of the information to be used or disclosed – for example, "laboratory results from July 1998" or "all health information";

2. The name or the person(s) or class of persons who are authorized to use or disclose the PHI;

3. The name or other specific identification of the person(s) or class of persons to whom the covered entity is authorized to make the requested use or disclosure;

4. The purpose for the requested use or disclosure;

5. The expiration date or event for the authorization; and

6. The signature of the individual or personal representative, date, and, if signed by a personal representative, a description of the personal representative's authority.

45 C.F.R. § 164.508(c)(1).

B. *Additional Required Statements.* In addition to the core elements listed above, an authorization must also contain the following statements:

1. An explanation of the individual's right to revoke the authorization or, if this is included in the privacy notice, a cross-reference to the privacy notice;

2. A statement describing the ability, or inability, of the covered entity to condition treatment, payment, enrollment, or eligibility for benefits based on whether or not the individual signs the authorization; and

3. A statement describing the potential for the information to be re-disclosed outside the protection of the medical privacy regulations.

45 C.F.R. § 164.508(c)(2).

C. *Advantages of an Authorization (from an Employer's Point of View).* An authorization allows an employer to have access to PHI without having to comply with all of the requirements in the medical privacy regulations.

1. This is particularly useful if the employer does not normally have access to PHI but needs PHI on an occasional basis for particular reasons.

2. For example, if an employee is having problems getting a plan's insurance carrier to pay a claim, it is not uncommon for the employee to ask his/her employer to help and many employers are willing to do so. Without an authorization, however, the employer will not be able to receive PHI from the insurance carrier without also becoming subject to the privacy requirements previously summarized. Many employers would perceive this as a high price to pay for trying to help one employee. Authorizations provide a way around this problem.

XIX. **Examples Illustrating the Application of the Rules.** The distinctions that the regulations make are difficult to grasp and apply, even for attorneys! For this reason, it might be helpful to provide a few examples. Please note that each of these examples assumes that the employer is not a "covered entity."

A. *Employee Talking to Fellow Employee.* An employee tells a coworker that she has cancer. The coworker is not a supervisor and does not have any responsibilities with respect to the employer's group health plan.

1. The bottom line is that the regulations will not limit the way in which the employer may use or disclose the information (although the employer should remember that other laws may apply).

2. Here's why: First, in our view the information is probably *not* PHI. To be PHI, the information must (among other things) be "created or received" by an employer. In this example, the information was shared between coworkers and the coworker receiving the information was not acting in an official capacity on behalf of the employer.

3. Second, assuming that the coworker is considered to be acting on behalf of the employer when receiving the information and that the information is therefore considered to be PHI, the employer did not receive the information in a way that would cause the information to be subject to restrictions.

4. An employer is indirectly subject to the regulations when it receives PHI from its group health plan or pursuant to the terms of a business associate agreement.

5. Aside from these two situations, an employer is not subject to the regulations, either directly or indirectly, and for that reason is not subject to any restrictions to the information which it may learn (although we would note that other laws may apply).

B. *Employee Talking to Supervisor.* The same employee tells her supervisor that she has cancer and may need to take some time off for treatment.

1. Again, the bottom line is that the regulations will not limit the way in which the employer may use or disclose the information (although the employer should remember that other laws may apply).

2. In our view, the information probably is PHI. Unlike the previous example, the information was shared with a supervisor for what appears to be a business-related reason (as opposed to being shared between friends). A supervisor normally acts on behalf of the employer with respect to the employees that are under his/her supervision. Thus, it would appear that the information was received "by the employer."

3. As in the first example, however, the employer did not receive the information in a way that would cause the employer to be indirectly subject to the regulations. The information was not received from the employer's group health plan and it was not received pursuant to a business associate agreement. For this reason, the regulations do not limit the way in which the employer may use or disclose the information (although other laws may apply).

C. *HR Director Overhears Information.* While sitting in the waiting room at the doctor's office, the HR director overhears a conversation between the doctor and a nurse in which the doctor says that the employee has cancer.

1. The bottom line in this example is the same as in the previous examples. In this example, the regulations will not limit the way in which the employer may use or disclose the information (although the employer should remember that other laws may apply). The analysis behind this conclusion is less straightforward, however.

2. First, we would note at the outset that the information was clearly PHI *as to the doctor and the nurse*.

   a. The doctor's office is a covered entity. As such, the doctor's office is required to have policies and procedures in place to prevent the unauthorized use or disclosure of patient information.

   b. The disclosure was apparently an inadvertent disclosure. Without knowing more about the steps the doctor's office took to prevent this type of inadvertent disclosure from occurring, it is not really possible to say whether or not the doctor has violated the regulations.

3. Whether the information is PHI *as to the employer* is not entirely clear under the regulations. In our view, it probably is not because the HR director was not acting in an official capacity when she received the information. But it could be argued that, regardless of how she learned the information, she has the authority to act on behalf of the company and the information is something that she now knows and is something that could influence the way she carries out her duties.

4. Assuming, however, that the information is PHI as to the employer, the regulations do not limit the way in which the information may be used or disclosed (although other laws may apply).

5. As in the previous examples, the employer did not receive the information in a way that would cause the information to be subject to restrictions. The employer did not receive the information from its group health plan or pursuant to a "business associate" agreement. Consequently, the employer is not subject to the regulations, directly or indirectly, with respect to the information.

D. *Doctor sends a letter to the employer.* Pursuant to a valid authorization signed by the employee, the doctor sends a letter to the HR director advising that the employee will need to be on "light duty" while she is being treated for cancer.

1. As in the previous examples, the regulations do not restrict the employer's use or disclosure of the information.

2. The information is PHI *as to the doctor.* Absent an authorization, the doctor would not be permitted to share that information with the employer. But, because a valid authorization was given, the regulations allow the doctor to disclose the information.

3. *As to the employer*, the information is also PHI. It is information that relates to the health of a specific individual and it is received by an employer.

4. Because the information was not received from the employer's group health plan or pursuant to a business associate contract, the employer's use and disclosure of the information is not restricted, directly or indirectly, by the regulations.

5. This does not mean that the employer is free to do whatever it wants with the information. Other laws may apply, just as they applied before the effective date of the privacy regulations. It does mean, however, that the employer is not subject to any restrictions stemming from the privacy regulations with respect to the information.

E. *CFO learns that the employee has cancer from reading a "large claims report."* In reviewing the periodic "large claims report" that is provided by the insurance company for the employer's group health plan, the CFO sees that the employee has incurred a large claim for the treatment of cancer.

1. Unlike the previous examples, the employer's use and disclosure of this information will be restricted by the regulations.

2. The information is clearly PHI because it relates to the health of a specific individual and it was received by the employer.

3. The employer is allowed to receive this type of information from its group health plan in some situations, but only if it agrees to restrictions on who is allowed to see it and how the information will be used (among other things).

4. Consequently, because the information came from the group health plan and because the employer agreed to restrictions on its use of the information as a prior condition to receiving the information, the employer's use of the information is required to be limited.

XX. **Enforcement.** HITECH heightened the enforcement of the privacy and security rules. In part, it requires HHS's Office of Civil Rights to conduct proactive audits of covered entities and business associates. Many agency-initiated compliance reviews stem from breach notifications and headline-grabbing events. This is a drastic change from government action based solely on the filing of individual complaints.

Moreover, state attorneys general are now authorized to bring civil enforcement action on behalf of state resident for violation of HIPAA privacy and security violations. Damages maybe obtained in those cases. See HITECH Act, 13410(e).

In addition, while individuals do not have a right to bring a private lawsuit to enforce the HIPAA privacy and security rules, the HITECH Act does give them the right to share in any monetary penalties collected as a result of the violation, if they can show they were harmed by the violation. This is similar to qui tam relators in a False Claims Act litigation, and is likely to incentivize many individuals to report HIPAA violations.

XXI. **Consequences of Non-Compliance.** The consequences of noncompliance with the medical privacy and security regulations can be serious.

A. There are civil penalties of up to $100 for each violation occurring prior to February 18, 2009. This is capped at a maximum of $25,000 per year for each type of violation. Social Security Act § 1176(a)(1); 42 U.S.C. § 1320d-5(a). These penalties, however, significantly increased under HITECH, only to be subsequently ratcheted down somewhat in April 2019. Civil penalties for violations on or after February 18, 2009 are based on the culpability or "state of mind" of the violator under a tiered approach. These penalties range from $100-$50,000 per violation of an identical requirement or prohibition where there is *no knowledge* of the violation (even if due diligence to discover the violation had been exercised) to a minimum $50,000 penalty per violation where the violator showed *willful neglect*.

While the cap was originally set at $1.5 million per calendar year for violations of for violations of an identical requirement or prohibition within the same calendar year (45 CFR §§ 160.401, 160.404(b)), this cap was significantly lowered in April 2019 in three of the four tiers. The 2019 enforcement policy provides for a $25,000 annual cap for a tier 1 violation (i.e., no knowledge) of an identical provision, a $100,000 annual cap for a tier 2 violation, a $250,000 annual cap for a tier 3 violation, and the policy retains the $1.5 million annual cap for a tier 4 violation. These amounts continue to be adjusted for inflation.

The money from the collected penalties goes to the Office of Civil Rights, to be used for HIPAA enforcement purposes. Subject to the issuance of regulations on methodology, harmed individuals are entitled to a percentage of the collected penalty. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009), § 13410(c).

B. Criminal penalties, including fines and imprisonment, may apply if a person "knowingly" discloses protected information in an improper manner. Social Security Act § 1177; 42 U.S.C. § 1320d-6.

C. The HITECH Act expressly authorizes all state attorneys general to bring civil actions in federal court for violations of HIPAA's administrative simplification provisions, to protect the interests of residents of their states. The actions may seek to enjoin activity in violation of HIPAA or to obtain damages on behalf of the state's residents. The amount of such damages is limited, however, to $100 for each violation, with a cap of $25,000 for identical violations during a calendar year.

D. Although the privacy regulations do not create a direct private cause of action, it may be possible for plan participants to bring a cause of action under other laws, such as ERISA.

XXII. **Preemption of State Laws.** The medical privacy regulations establish a "floor" but not a "ceiling." As a general proposition, states are free to enact laws that are more strict and demanding than the medical privacy regulations. Social Security Act § 1178; 42 U.S.C. § 1320d-7. Because, however, ERISA preempts state law with respect to ERISA plans (ERISA § 514), it is not clear whether ERISA group health plans can be required to comply with stricter state laws.

XXIII. **Electronic Data Interchange ("EDI").** Covered entities that engage in certain "covered transactions" will be required to comply with rules that are designed to standardize the format and content of their electronic transactions. 45 C.F.R. § 162.923.

A. *Covered Transactions.* The following transactions are subject to the EDI rules:

1. Health claims and equivalent encounter information;

2. Health care payment and remittance advice;

3. Coordination of benefits;

4. Health claim status;

5. Enrollment and disenrollment in a health plan;

6. Eligibility for a health plan;

7. Health plan premium payments;

8. Referral certification and authorization;

9. First report of injury; and

10. Health claims attachments.

45 C.F.R. § 162.1000 *et seq.*

B. *Application to Employers with Group Health Plans.* The application of the EDI regulations to employers with group health plans is not entirely clear.

1. In drafting the EDI regulations, HHS's focus was on transactions between health care providers and persons who process and pay claims. There is no indication that the drafters were concerned with communications between an employer sponsoring a group health plan and the insurance company for that plan, for example.

2. As drafted, however, the EDI regulations apply to group health plans and the list of covered transactions includes "enrollment and disenrollment in a health plan" and "health plan premium payments."

3. The processing of enrollment and disenrollment information and the payment of premiums is generally carried out by the employer, in most situations. The employer is not a covered entity, and, for that reason, is not subject to the EDI regulations.

4. Consequently, we may need more guidance, either formal or informal, from HHS before we know what most employers will need to do to comply with the EDI regulations.

C. *Deadline for Compliance.* The deadline for complying with the EDI regulations was October 16, 2002, subject to two exceptions:

1. Large plans and other covered entities were entitled to an automatic one-year extension if that extension was requested no later than October 15, 2002. Thus, if an extension was requested before the deadline, the compliance date was extended to October 16, 2003.

2. Small plans were required to comply as of October 16, 2003. Small plans were automatically given an extra year to comply and were not required to request an extension.

45 C.F.R. § 162.900.

XXIV. **What are the Key Deadlines for Most Employers?** The key deadlines that will affect most employers are shown on the attached sheet.

IMPORTANT NOTE

Please note that this is a brief summary of an exceptionally lengthy and complicated regulation. Our intent has been to highlight provisions that are likely to affect employers who are sponsors of group health plans. Employers who are involved with PHI in other ways – for example, employers that are also healthcare providers – will be subject to additional requirements. Accordingly, employers are advised not to rely on this outline. Rather, employers should obtain advice from a competent professional as to how the HIPAA medical privacy and security regulations will apply to them in light of their facts and circumstances.

HIPAA MEDICAL PRIVACY REGULATIONS
KEY COMPLIANCE DATES FOR EMPLOYERS OFFERING GROUP HEALTH PLANS

Date	*What is it?*	*Who is Affected?*
April 14, 2003	Effective Date for Privacy Rules (with a special transition rule for business associate contracts)	All "***covered entities***" except "***small plans***"
October 16, 2003	Compliance Date for HIPAA's electronic transaction (or "EDI") requirements (with compliance dates in 2012, 2013 and 2014 for subsequently issued interim final regulations)	***"Small plans"*** and any other ***"covered entities"*** that requested an extension prior to the October 15, 2002, deadline if they transmit health information in electronic form in connection with one or more ***"standard transactions"*** for which the Department of Health and Human Services has prescribed the use of standard data formats and codes
April 14, 2004	Effective Date for Privacy Rules for "***small plans***"	"***Small plans***"
April 20, 2005	Effective Date for Security Rules	All "***covered entities***" except "***small plans***"
April 20, 2006	Effective Date for Security Rules for "***small plans***"	"***Small plans***"
September 23, 2009 through September 22, 2013	Period during which Interim Final Regulations regarding HITECH's breach notification rules are effective	All "***covered entities***" and business associates
March 26, 2013	Effective Date for Increased Civil Monetary Penalties	All "***covered entities***" and business associates
September 23, 2013	Effective Date for Final Breach Notification Rules	All "***covered entities***" and business associates
September 23, 2013	Effective Date for Compliance with Modifications to Privacy, Security and Enforcement Rules under HITECH	All "***covered entities***" and business associates (with delayed effective date to amend many business associate contracts)
April 23, 2019	Effective date of the decrease in the maximum annual penalty amounts for HIPAA violations under tiers 1 through 3.	All "***covered entities***" and business associates

U.S. Department of Health and Human Services
Office for Civil Rights

HIPAA Administrative Simplification

Regulation Text

45 CFR Parts 160, 162, and 164
(Unofficial Version, as amended through March 26, 2013)

HIPAA Administrative Simplification

Table of Contents

Section **Page**

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS.....10

SUBPART A—GENERAL PROVISIONS 10

§ 160.101 Statutory basis and purpose.....10

§ 160.102 Applicability. 11

§ 160.103 Definitions.....11

§ 160.104 Modifications.....17

§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.....17

SUBPART B—PREEMPTION OF STATE LAW..... 17

§ 160.201 Statutory basis.....17

§ 160.202 Definitions.....18

§ 160.203 General rule and exceptions.....18

§ 160.204 Process for requesting exception determinations. 19

§ 160.205 Duration of effectiveness of exception determinations. 19

SUBPART C—COMPLIANCE AND INVESTIGATIONS..... 19

§ 160.300 Applicability. 19

§ 160.302 [Reserved].....20

§ 160.304 Principles for achieving compliance. 20

§ 160.306 Complaints to the Secretary.....20

§ 160.308 Compliance reviews. 20

§ 160.310 Responsibilities of covered entities and business associates. 20

§ 160.312 Secretarial action regarding complaints and compliance reviews. 21

§ 160.314 Investigational subpoenas and inquiries. 21

§ 160.316 Refraining from intimidation or retaliation. 23

SUBPART D—IMPOSITION OF CIVIL MONEY PENALTIES 23

§ 160.400 Applicability. 23

§ 160.401 Definitions. 23

§ 160.402 Basis for a civil money penalty. 23

§ 160.404 Amount of a civil money penalty. 24

§ 160.406 Violations of an identical requirement or prohibition. 24

§ 160.408 Factors considered in determining the amount of a civil money penalty. 25

§ 160.410 Affirmative defenses. 25

§ 160.412 Waiver 26

§ 160.414 Limitations. 26

§ 160.416 Authority to settle. 26

§ 160.418 Penalty not exclusive. 26

§ 160.420 Notice of proposed determination. 26

§ 160.422 Failure to request a hearing. 26

§ 160.424 Collection of penalty. 27

§ 160.426 Notification of the public and other agencies. 27

SUBPART E—PROCEDURES FOR HEARINGS 27

§ 160.500 Applicability. 27

§ 160.502 Definitions. 27

§ 160.504 Hearing before an ALJ. 27

§ 160.506 Rights of the parties. 28

§ 160.508 Authority of the ALJ. 28

§ 160.510 Ex parte contacts. 29

§ 160.512 Prehearing conferences. 29

§ 160.514 Authority to settle. 29

§ 160.516 Discovery. 29

§ 160.518 Exchange of witness lists, witness statements, and exhibits. 30

§ 160.520 Subpoenas for attendance at hearing. 30

§ 160.522 Fees. 31

§ 160.524 Form, filing, and service of papers. 31

§ 160.526 Computation of time. 31

§ 160.528 Motions. 31

§ 160.530 Sanctions. 32

§ 160.532 Collateral estoppel. 32

§ 160.534 The hearing. 32

§ 160.536 Statistical sampling. 33

§ 160.538 Witnesses. 33

§ 160.540 Evidence. 33

§ 160.542 The record. 34

§ 160.544 Post hearing briefs. 34

§ 160.546 ALJ's decision. 34

§ 160.548 Appeal of the ALJ's decision. 34

§ 160.550 Stay of the Secretary's decision. 35

PART 162—ADMINISTRATIVE REQUIREMENTS 37

SUBPART A—GENERAL PROVISIONS 38

§ 162.100 Applicability. 38

§ 162.103 Definitions. 38

SUBPARTS B-C [RESERVED] 39

SUBPART D—STANDARD UNIQUE HEALTH IDENTIFIER FOR HEALTH CARE PROVIDERS 39

§ 162.402 [Reserved] 39

§ 162.404 Compliance dates of the implementation of the standard unique health identifier for health care providers. 39

§ 162.406 Standard unique health identifier for health care providers. 39

§ 162.408 National Provider System. 39

§ 162.410 Implementation specifications: Health care providers. 40

§ 162.412 Implementation specifications: Health plans. 40

§ 162.414 Implementation specifications: Health care clearinghouses. 40

SUBPART E—STANDARD UNIQUE HEALTH IDENTIFIER FOR HEALTH PLANS 40

§ 162.502 [Reserved] 40

§ 162.504 Compliance requirements for the implementation of the standard unique health plan identifier. 40

§ 162.506 Standard unique health plan identifier. 41

§ 162.508 Enumeration System. 41

§ 162.510 Full implementation requirements: Covered entities. 41

§ 162.512 Implementation specifications: Health plans. 41

§ 162.514 Other entity identifier. 42

SUBPART F—STANDARD UNIQUE EMPLOYER IDENTIFIER 42

§ 162.600 Compliance dates of the implementation of the standard unique employer identifier. 42

§ 162.605 Standard unique employer identifier. 42

§ 162.610 Implementation specifications for covered entities. 42

SUBPARTS G-H [RESERVED] 42

SUBPART I—GENERAL PROVISIONS FOR TRANSACTIONS 42

§ 162.900 [Reserved] 42

§ 162.910 Maintenance of standards and adoption of modifications and new standards. 42

§ 162.915 Trading partner agreements. 43

§ 162.920 Availability of implementation specifications and operating rules. 43

§ 162.923 Requirements for covered entities. 46

§ 162.925 Additional requirements for health plans. 47

§ 162.930 Additional rules for health care clearinghouses. 47

§ 162.940 Exceptions from standards to permit testing of proposed modifications. 48

SUBPART J—CODE SETS 49

§ 162.1000 General requirements. 49

§ 162.1002 Medical data code sets. 49

§ 162.1011 Valid code sets. 50

SUBPART K—HEALTH CARE CLAIMS OR EQUIVALENT ENCOUNTER INFORMATION 50

§ 162.1101 Health care claims or equivalent encounter information transaction. 50

§ 162.1102 Standards for health care claims or equivalent encounter information transaction. 50

SUBPART L—ELIGIBILITY FOR A HEALTH PLAN 52

§ 162.1201 Eligibility for a health plan transaction. 52

§ 162.1202 Standards for eligibility for a health plan transaction. 52

§ 162.1203 Operating rules for eligibility for a health plan transaction. 52

SUBPART M—REFERRAL CERTIFICATION AND AUTHORIZATION 53

§ 162.1301 Referral certification and authorization transaction. 53

§ 162.1302 Standards for referral certification and authorization transaction. 53

SUBPART N—HEALTH CARE CLAIM STATUS 54

§ 162.1401 Health care claim status transaction. 54

§ 162.1402 Standards for health care claim status transaction. 54

§ 162.1403 Operating rules for health care claim status transaction. 54

SUBPART O—ENROLLMENT AND DISENROLLMENT IN A HEALTH PLAN 54

§ 162.1501 Enrollment and disenrollment in a health plan transaction. 54

§ 162.1502 Standards for enrollment and disenrollment in a health plan transaction. 54

SUBPART P—HEALTH CARE ELECTRONIC FUNDS TRANSFERS (EFT) AND REMITTANCE ADVICE 55

§ 162.1601 Health care electronic funds transfers (EFT) and remittance advice transaction. 55

§ 162.1602 Standards for health care electronic funds transfers (EFT) and remittance advice transaction. 55

§ 162.1603 Operating rules for health care electronic funds transfers (EFT) and remittance advice transaction. 56

SUBPART Q—HEALTH PLAN PREMIUM PAYMENTS 56

§ 162.1701 Health plan premium payments transaction. 56

§ 162.1702 Standards for health plan premium payments transaction. 56

SUBPART R—COORDINATION OF BENEFITS 57

§ 162.1801 Coordination of benefits transaction. 57

§ 162.1802 Standards for coordination of benefits information transaction. 57

SUBPART S—MEDICAID PHARMACY SUBROGATION 58

§ 162.1901 Medicaid pharmacy subrogation transaction. 58

§ 162.1902 Standard for Medicaid pharmacy subrogation transaction. 58

PART 164—SECURITY AND PRIVACY 59

SUBPART A—GENERAL PROVISIONS 59

§ 164.102 Statutory basis. 59

§ 164.103 Definitions. 59

§ 164.104 Applicability. 60

§ 164.105 Organizational requirements. 60

§ 164.106 Relationship to other parts. 62

SUBPART B [RESERVED] 62

SUBPART C—SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION 62

§ 164.302 Applicability. 62

§ 164.304 Definitions. 62

§ 164.306 Security standards: General rules. 63

§ 164.308 Administrative safeguards. 64

§ 164.310 Physical safeguards. 66

§ 164.312 Technical safeguards. 66

§ 164.314 Organizational requirements. 67

§ 164.316 Policies and procedures and documentation requirements. 68

§ 164.318 Compliance dates for the initial implementation of the security standards. 68

SUBPART D—NOTIFICATION IN THE CASE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION 71

§ 164.400 Applicability. 71

§ 164.402 Definitions. 71

§ 164.404 Notification to individuals. 71

§ 164.406 Notification to the media. 72

§ 164.408 Notification to the Secretary. 72

§ 164.410 Notification by a business associate. 73

§ 164.412 Law enforcement delay. 73

§ 164.414 Administrative requirements and burden of proof 73

SUBPART E—PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 73

§ 164.500 Applicability. 73

§ 164.501 Definitions. 74

§ 164.502 Uses and disclosures of protected health information: General rules. 77

§ 164.504 Uses and disclosures: Organizational requirements. 81

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. 84

§ 164.508 Uses and disclosures for which an authorization is required. 85

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object. 87

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required. 88

§ 164.514 Other requirements relating to uses and disclosures of protected health information. 96

§ 164.520 Notice of privacy practices for protected health information. 101

§ 164.522 Rights to request privacy protection for protected health information. 104

§ 164.524 Access of individuals to protected health information. 105

§ 164.526 Amendment of protected health information. 108

§ 164.528 Accounting of disclosures of protected health information. 110

§ 164.530 Administrative requirements. 111

§ 164.532 Transition provisions. 114

§ 164.534 Compliance dates for initial implementation of the privacy standards. 115

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

Contents

Subpart A—General Provisions

§ 160.101 Statutory basis and purpose.
§ 160.102 Applicability.
§ 160.103 Definitions.
§ 160.104 Modifications.
§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.

Subpart B—Preemption of State Law

§ 160.201 Statutory basis.
§ 160.202 Definitions.
§ 160.203 General rule and exceptions.
§ 160.204 Process for requesting exception determinations.
§ 160.205 Duration of effectiveness of exception determinations.

Subpart C—Compliance and Investigations

§ 160.300 Applicability.
§ 160.302 [Reserved]
§ 160.304 Principles for achieving compliance.
§ 160.306 Complaints to the Secretary.
§ 160.308 Compliance reviews.
§ 160.310 Responsibilities of covered entities and business associates.
§ 160.312 Secretarial action regarding complaints and compliance reviews.
§ 160.314 Investigational subpoenas and inquiries.
§ 160.316 Refraining from intimidation or retaliation.

Subpart D—Imposition of Civil Money Penalties

§ 160.400 Applicability.
§ 160.401 Definitions.
§ 160.402 Basis for a civil money penalty.
§ 160.404 Amount of a civil money penalty.
§ 160.406 Violations of an identical requirement or prohibition.
§ 160.408 Factors considered in determining the amount of a civil money penalty.
§ 160.410 Affirmative defenses.
§ 160.412 Waiver.
§ 160.414 Limitations.
§ 160.416 Authority to settle.
§ 160.418 Penalty not exclusive.
§ 160.420 Notice of proposed determination.
§ 160.422 Failure to request a hearing.
§ 160.424 Collection of penalty.
§ 160.426 Notification of the public and other agencies.

Subpart E—Procedures for Hearings

§ 160.500 Applicability.
§ 160.502 Definitions.
§ 160.504 Hearing before an ALJ.
§ 160.506 Rights of the parties.
§ 160.508 Authority of the ALJ.
§ 160.510 Ex parte contacts.
§ 160.512 Prehearing conferences.
§ 160.514 Authority to settle.
§ 160.516 Discovery.
§ 160.518 Exchange of witness lists, witness statements, and exhibits.
§ 160.520 Subpoenas for attendance at hearing.
§ 160.522 Fees.
§ 160.524 Form, filing, and service of papers.
§ 160.526 Computation of time.
§ 160.528 Motions.
§ 160.530 Sanctions.
§ 160.532 Collateral estoppel.
§ 160.534 The hearing.
§ 160.536 Statistical sampling.
§ 160.538 Witnesses.
§ 160.540 Evidence.
§ 160.542 The record.
§ 160.544 Post hearing briefs.
§ 160.546 ALJ's decision.
§ 160.548 Appeal of the ALJ's decision.
§ 160.550 Stay of the Secretary's decision.
§ 160.552 Harmless error.

AUTHORITY: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); 5 U.S.C. 552; secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279; and sec. 1104 of Pub. L. 111-148, 124 Stat. 146-154.

SOURCE: 65 FR 82798, Dec. 28, 2000, unless otherwise noted.

Subpart A—General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

[78 FR 5687, Jan. 25, 2013]

§ 160.102 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

(c) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 78 FR 5687, Jan. 25, 2013]

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

Administrative simplification provision means any requirement or prohibition established by:

(1) 42 U.S.C. 1320d-1320d-4, 1320d-7, 1320d-8, and 1320d-9;

(2) Section 264 of Pub. L. 104-191;

(3) Sections 13400-13424 of Public Law 111-5; or

(4) This subchapter.

ALJ means Administrative Law Judge.

ANSI stands for the American National Standards Institute.

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance

issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Civil money penalty or *penalty* means the amount determined under § 160.404 of this part and includes the plural of these terms.

CMS stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services.

Compliance date means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.

(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

Electronic media means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of *protected health information* as specified in this section.

Employer is defined as it is in 26 U.S.C. 3401(d).

Family member means, with respect to an individual:

(1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or

(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one

parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Genetic information means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual.

Genetic services means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education.

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data

elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq*.

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq*.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq*.

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Manifestation or *manifested* means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Person means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

Respondent means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services, or practices:

(i) Classification of components;

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of protected health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Health care electronic funds transfers (EFT) and remittance advice.

(12) Other transactions that the Secretary may prescribe by regulation.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Violation or *violate* means, as the context may require, failure to comply with an administrative simplification provision.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002; 67 FR 53266, Aug. 14, 2002; 68 FR 8374, Feb. 20, 2003; 71 FR 8424, Feb. 16, 2006; 76 FR 40495, July 8, 2011; 77 FR 1589, Jan. 10, 2012; 78 FR 5687, Jan. 25, 2013]

§ 160.104 Modifications.

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.

(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.

(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002]

§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.

Except as otherwise provided, with respect to rules that adopt new standards and implementation specifications or modifications to standards and implementation specifications in this subchapter in accordance with § 160.104 that become effective after January 25, 2013, covered entities and business associates must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications.

[78 FR 5689, Jan. 25, 2013]

Subpart B—Preemption of State Law

§ 160.201 Statutory basis.

The provisions of this subpart implement section 1178 of the Act, section 262 of Public Law 104-191, section 264(c) of Public Law 104-191, and section 13421(a) of Public Law 111-5.

[78 FR 5689, Jan. 25, 2013]

§ 160.202 Definitions.

For purposes of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 74 FR 42767, Aug. 24, 2009; 78 FR 5689, Jan. 25, 2013]

§ 160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002]

§ 160.204 Process for requesting exception determinations.

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

(1) The State law for which the exception is requested;

(2) The particular standard, requirement, or implementation specification for which the exception is requested;

(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

(4) How health care providers, health plans, and other entities would be affected by the exception;

(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

(6) Any other information the Secretary may request in order to make the determination.

(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the FEDERAL REGISTER. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.

(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

§ 160.205 Duration of effectiveness of exception determinations.

An exception granted under this subpart remains in effect until:

(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

Subpart C—Compliance and Investigations

SOURCE: 71 FR 8424, Feb. 16, 2006, unless otherwise noted.

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, business associates, and others with respect to ascertaining the compliance by covered entities and business associates with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.

[78 FR 5690, Jan. 25, 2013]

§ 160.302 [Reserved]

§ 160.304 Principles for achieving compliance.

(a) *Cooperation.* The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered entities and business associates in obtaining compliance with the applicable administrative simplification provisions.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the applicable administrative simplification provisions.

[78 FR 5690, Jan. 25, 2013]

§ 160.306 Complaints to the Secretary.

(a) *Right to file a complaint.* A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary.

(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s).

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.

(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the FEDERAL REGISTER.

(c) *Investigation.* (1) The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.

(2) The Secretary may investigate any other complaint filed under this section.

(3) An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation.

(4) At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

[71 FR 8424, Feb. 16, 2006, as amended at 78 FR 5690, Jan. 25, 2013]

§ 160.308 Compliance reviews.

(a) The Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

(b) The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions in any other circumstance.

[78 FR 5690, Jan. 25, 2013]

§ 160.310 Responsibilities of covered entities and business associates.

(a) *Provide records and compliance reports.* A covered entity or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions.

(c) *Permit access to information.* (1) A covered entity or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity or business associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

[78 FR 5690, Jan. 25, 2013]

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) *Resolution when noncompliance is indicated.* (1) If an investigation of a complaint pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.

(2) If the matter is resolved by informal means, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

(3) If the matter is not resolved by informal means, the Secretary will—

(i) So inform the covered entity or business associate and provide the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under §§ 160.408 and 160.410 of this part. The covered entity or business associate must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of such notification; and

(ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity or business associate of such finding in a notice of proposed determination in accordance with § 160.420 of this part.

(b) *Resolution when no violation is found.* If, after an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

[78 FR 5690, Jan. 25, 2013]

§ 160.314 Investigational subpoenas and inquiries.

(a) The Secretary may issue subpoenas in accordance with 42 U.S.C. 405(d) and (e), 1320a-7a(j), and 1320d-5 to require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review pursuant to this part. For purposes of this paragraph, a person other than a natural person is termed an "entity."

(1) A subpoena issued under this paragraph must—

(i) State the name of the person (including the entity, if applicable) to whom the subpoena is addressed;

(ii) State the statutory authority for the subpoena;

(iii) Indicate the date, time, and place that the testimony will take place;

(iv) Include a reasonably specific description of any

documents or items required to be produced; and

(v) If the subpoena is addressed to an entity, describe with reasonable particularity the subject matter on which testimony is required. In that event, the entity must designate one or more natural persons who will testify on its behalf, and must state as to each such person that person's name and address and the matters on which he or she will testify. The designated person must testify as to matters known or reasonably available to the entity.

(2) A subpoena under this section must be served by—

(i) Delivering a copy to the natural person named in the subpoena or to the entity named in the subpoena at its last principal place of business; or

(ii) Registered or certified mail addressed to the natural person at his or her last known dwelling place or to the entity at its last known principal place of business.

(3) A verified return by the natural person serving the subpoena setting forth the manner of service or, in the case of service by registered or certified mail, the signed return post office receipt, constitutes proof of service.

(4) Witnesses are entitled to the same fees and mileage as witnesses in the district courts of the United States (28 U.S.C. 1821 and 1825). Fees need not be paid at the time the subpoena is served.

(5) A subpoena under this section is enforceable through the district court of the United States for the district where the subpoenaed natural person resides or is found or where the entity transacts business.

(b) Investigational inquiries are non-public investigational proceedings conducted by the Secretary.

(1) Testimony at investigational inquiries will be taken under oath or affirmation.

(2) Attendance of non-witnesses is discretionary with the Secretary, except that a witness is entitled to be accompanied, represented, and advised by an attorney.

(3) Representatives of the Secretary are entitled to attend and ask questions.

(4) A witness will have the opportunity to clarify his or her answers on the record following questioning by the Secretary.

(5) Any claim of privilege must be asserted by the witness on the record.

(6) Objections must be asserted on the record. Errors of any kind that might be corrected if promptly presented will be deemed to be waived unless reasonable objection is made at the investigational inquiry. Except where the objection is on the grounds of privilege, the question will be answered on the record, subject to objection.

(7) If a witness refuses to answer any question not privileged or to produce requested documents or items, or engages in conduct likely to delay or obstruct the investigational inquiry, the Secretary may seek enforcement of the subpoena under paragraph (a)(5) of this section.

(8) The proceedings will be recorded and transcribed. The witness is entitled to a copy of the transcript, upon payment of prescribed costs, except that, for good cause, the witness may be limited to inspection of the official transcript of his or her testimony.

(9)(i) The transcript will be submitted to the witness for signature.

(A) Where the witness will be provided a copy of the transcript, the transcript will be submitted to the witness for signature. The witness may submit to the Secretary written proposed corrections to the transcript, with such corrections attached to the transcript. If the witness does not return a signed copy of the transcript or proposed corrections within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of its being submitted to him or her for signature, the witness will be deemed to have agreed that the transcript is true and accurate.

(B) Where, as provided in paragraph (b)(8) of this section, the witness is limited to inspecting the transcript, the witness will have the opportunity at the time of inspection to propose corrections to the transcript, with corrections attached to the transcript. The witness will also have the opportunity to sign the transcript. If the witness does not sign the transcript or offer corrections within 30 days (computed in the same manner

as prescribed under § 160.526 of this part) of receipt of notice of the opportunity to inspect the transcript, the witness will be deemed to have agreed that the transcript is true and accurate.

(ii) The Secretary's proposed corrections to the record of transcript will be attached to the transcript.

(c) Consistent with § 160.310(c)(3), testimony and other evidence obtained in an investigational inquiry may be used by HHS in any of its activities and may be used or offered into evidence in any administrative or judicial proceeding.

§ 160.316 Refraining from intimidation or retaliation.

A covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for—

(a) Filing of a complaint under § 160.306;

(b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under this part; or

(c) Opposing any act or practice made unlawful by this subchapter, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of subpart E of part 164 of this subchapter.

[71 FR 8426, Feb. 16, 2006, as amended at 78 FR 5691, Jan. 25, 2013]

Subpart D—Imposition of Civil Money Penalties

SOURCE: 71 FR 8426, Feb. 16, 2006, unless otherwise noted.

§ 160.400 Applicability.

This subpart applies to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.

§ 160.401 Definitions.

As used in this subpart, the following terms have the following meanings:

Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

[74 FR 56130, Oct. 30, 2009, as amended at 78 FR 5691, Jan. 25, 2013]

§ 160.402 Basis for a civil money penalty.

(a) *General rule.* Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision.

(b) *Violation by more than one covered entity or business associate.* (1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate.

(2) A covered entity that is a member of an affiliated covered entity, in accordance with § 164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter based on an act or omission of the affiliated covered entity, unless it is established that another member of the affiliated covered entity was responsible for the violation.

(c) *Violation attributed to a covered entity or business associate.* (1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.

(2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

[78 FR 5691, Jan. 25, 2013]

§ 160.404 Amount of a civil money penalty.

(a) The amount of a civil money penalty will be determined in accordance with paragraph (b) of this section and §§ 160.406, 160.408, and 160.412.

(b) The amount of a civil money penalty that may be imposed is subject to the following limitations:

(1) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty—

(i) In the amount of more than $100 for each violation; or

(ii) In excess of $25,000 for identical violations during a calendar year (January 1 through the following December 31);

(2) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty—

(i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision,

(A) In the amount of less than $100 or more than $50,000 for each violation; or

(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(ii) For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect,

(A) In the amount of less than $1,000 or more than $50,000 for each violation; or

(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

(A) In the amount of less than $10,000 or more than $50,000 for each violation; or

(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

(A) In the amount of less than $50,000 for each violation; or

(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31).

(3) If a requirement or prohibition in one administrative simplification provision is repeated in a more general form in another administrative simplification provision in the same subpart, a civil money penalty may be imposed for a violation of only one of these administrative simplification provisions.

[71 FR 8426, Feb. 16, 2006, as amended at 74 FR 56130, Oct. 30, 2009; 78 FR 5691, Jan. 25, 2013]

§ 160.406 Violations of an identical requirement or prohibition.

The Secretary will determine the number of violations of an administrative simplification provision based on the nature of the covered entity's or business associate's obligation to act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision.

[78 FR 5691, Jan. 25, 2013]

§ 160.408 Factors considered in determining the amount of a civil money penalty.

In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:

(a) The nature and extent of the violation, consideration of which may include but is not limited to:

(1) The number of individuals affected; and

(2) The time period during which the violation occurred;

(b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

(1) Whether the violation caused physical harm;

(2) Whether the violation resulted in financial harm;

(3) Whether the violation resulted in harm to an individual's reputation; and

(4) Whether the violation hindered an individual's ability to obtain health care;

(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the current violation is the same or similar to previous indications of noncompliance;

(2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

(3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

(4) How the covered entity or business associate has responded to prior complaints;

(d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

(3) The size of the covered entity or business associate; and

(e) Such other matters as justice may require.

[78 FR 5691, Jan. 25, 2013]

§ 160.410 Affirmative defenses.

(a) The Secretary may not:

(1) Prior to February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that the violation is punishable under 42 U.S.C. 1320d-6.

(2) On or after February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that a penalty has been imposed under 42 U.S.C. 1320d-6 with respect to such act.

(b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:

(1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or

(2) The violation is—

(i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated and is not due to willful neglect; and

(ii) Corrected during either:

(A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or

(B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

(c) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of the Secretary that the violation is—

(1) Not due to willful neglect; and

(2) Corrected during either:

(i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or

(ii) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

[78 FR 5692, Jan. 25, 2013]

§ 160.412 Waiver.

For violations described in § 160.410(b)(2) or (c) that are not corrected within the period specified under such paragraphs, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation.

[8 FR 5692, Jan. 25, 2013]

§ 160.414 Limitations.

No action under this subpart may be entertained unless commenced by the Secretary, in accordance with § 160.420, within 6 years from the date of the occurrence of the violation.

§ 160.416 Authority to settle.

Nothing in this subpart limits the authority of the Secretary to settle any issue or case or to compromise any penalty.

§ 160.418 Penalty not exclusive.

Except as otherwise provided by 42 U.S.C. 1320d-5(b)(1) and 42 U.S.C. 299b-22(f)(3), a penalty imposed under this part is in addition to any other penalty prescribed by law.

[78 FR 5692, Jan. 25, 2013]

§ 160.420 Notice of proposed determination.

(a) If a penalty is proposed in accordance with this part, the Secretary must deliver, or send by certified mail with return receipt requested, to the respondent, written notice of the Secretary's intent to impose a penalty. This notice of proposed determination must include—

(1) Reference to the statutory basis for the penalty;

(2) A description of the findings of fact regarding the violations with respect to which the penalty is proposed (except that, in any case where the Secretary is relying upon a statistical sampling study in accordance with § 160.536 of this part, the notice must provide a copy of the study relied upon by the Secretary);

(3) The reason(s) why the violation(s) subject(s) the respondent to a penalty;

(4) The amount of the proposed penalty and a reference to the subparagraph of § 160.404 upon which it is based.

(5) Any circumstances described in § 160.408 that were considered in determining the amount of the proposed penalty; and

(6) Instructions for responding to the notice, including a statement of the respondent's right to a hearing, a statement that failure to request a hearing within 90 days permits the imposition of the proposed penalty without the right to a hearing under § 160.504 or a right of appeal under § 160.548 of this part, and the address to which the hearing request must be sent.

(b) The respondent may request a hearing before an ALJ on the proposed penalty by filing a request in accordance with § 160.504 of this part.

[71 FR 8426, Feb. 16, 2006, as amended at 74 FR 56131, Oct. 30, 2009]

§ 160.422 Failure to request a hearing.

If the respondent does not request a hearing within the time prescribed by § 160.504 of this

part and the matter is not settled pursuant to § 160.416, the Secretary will impose the proposed penalty or any lesser penalty permitted by 42 U.S.C. 1320d-5. The Secretary will notify the respondent by certified mail, return receipt requested, of any penalty that has been imposed and of the means by which the respondent may satisfy the penalty, and the penalty is final on receipt of the notice. The respondent has no right to appeal a penalty under § 160.548 of this part with respect to which the respondent has not timely requested a hearing.

§ 160.424 Collection of penalty.

(a) Once a determination of the Secretary to impose a penalty has become final, the penalty will be collected by the Secretary, subject to the first sentence of 42 U.S.C. 1320a-7a(f).

(b) The penalty may be recovered in a civil action brought in the United States district court for the district where the respondent resides, is found, or is located.

(c) The amount of a penalty, when finally determined, or the amount agreed upon in compromise, may be deducted from any sum then or later owing by the United States, or by a State agency, to the respondent.

(d) Matters that were raised or that could have been raised in a hearing before an ALJ, or in an appeal under 42 U.S.C. 1320a-7a(e), may not be raised as a defense in a civil action by the United States to collect a penalty under this part.

§ 160.426 Notification of the public and other agencies.

Whenever a proposed penalty becomes final, the Secretary will notify, in such manner as the Secretary deems appropriate, the public and the following organizations and entities thereof and the reason it was imposed: the appropriate State or local medical or professional organization, the appropriate State agency or agencies administering or supervising the administration of State health care programs (as defined in 42 U.S.C. 1320a-7(h)), the appropriate utilization and quality control peer review organization, and the appropriate State or local licensing agency or organization (including the agency specified in 42 U.S.C. 1395aa(a), 1396a(a)(33)).

Subpart E—Procedures for Hearings

SOURCE: 71 FR 8428, Feb. 16, 2006, unless otherwise noted.

§ 160.500 Applicability.

This subpart applies to hearings conducted relating to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.

§ 160.502 Definitions.

As used in this subpart, the following term has the following meaning:

Board means the members of the HHS Departmental Appeals Board, in the Office of the Secretary, who issue decisions in panels of three.

§ 160.504 Hearing before an ALJ.

(a) A respondent may request a hearing before an ALJ. The parties to the hearing proceeding consist of—

(1) The respondent; and

(2) The officer(s) or employee(s) of HHS to whom the enforcement authority involved has been delegated.

(b) The request for a hearing must be made in writing signed by the respondent or by the respondent's attorney and sent by certified mail, return receipt requested, to the address specified in the notice of proposed determination. The request for a hearing must be mailed within 90 days after notice of the proposed determination is received by the respondent. For purposes of this section, the respondent's date of receipt of the notice of proposed determination is presumed to be 5 days after the date of the notice unless the respondent makes a reasonable showing to the contrary to the ALJ.

(c) The request for a hearing must clearly and directly admit, deny, or explain each of the findings of fact contained in the notice of proposed determination with regard to which the respondent has any knowledge. If the respondent has no knowledge of a particular finding of fact and so states, the finding shall be deemed denied. The request for a hearing must also state the circumstances or arguments that the respondent alleges constitute the grounds for any defense and the factual and legal basis for opposing the penalty, except that a respondent may raise an affirmative defense

under § 160.410(b)(1) at any time.

(d) The ALJ must dismiss a hearing request where—

(1) On motion of the Secretary, the ALJ determines that the respondent's hearing request is not timely filed as required by paragraphs (b) or does not meet the requirements of paragraph (c) of this section;

(2) The respondent withdraws the request for a hearing;

(3) The respondent abandons the request for a hearing; or

(4) The respondent's hearing request fails to raise any issue that may properly be addressed in a hearing.

§ 160.506 Rights of the parties.

(a) Except as otherwise limited by this subpart, each party may—

(1) Be accompanied, represented, and advised by an attorney;

(2) Participate in any conference held by the ALJ;

(3) Conduct discovery of documents as permitted by this subpart;

(4) Agree to stipulations of fact or law that will be made part of the record;

(5) Present evidence relevant to the issues at the hearing;

(6) Present and cross-examine witnesses;

(7) Present oral arguments at the hearing as permitted by the ALJ; and

(8) Submit written briefs and proposed findings of fact and conclusions of law after the hearing.

(b) A party may appear in person or by a representative. Natural persons who appear as an attorney or other representative must conform to the standards of conduct and ethics required of practitioners before the courts of the United States.

(c) Fees for any services performed on behalf of a party by an attorney are not subject to the provisions of 42 U.S.C. 406, which authorizes the Secretary to specify or limit their fees.

§ 160.508 Authority of the ALJ.

(a) The ALJ must conduct a fair and impartial hearing, avoid delay, maintain order, and ensure that a record of the proceeding is made.

(b) The ALJ may—

(1) Set and change the date, time and place of the hearing upon reasonable notice to the parties;

(2) Continue or recess the hearing in whole or in part for a reasonable period of time;

(3) Hold conferences to identify or simplify the issues, or to consider other matters that may aid in the expeditious disposition of the proceeding;

(4) Administer oaths and affirmations;

(5) Issue subpoenas requiring the attendance of witnesses at hearings and the production of documents at or in relation to hearings;

(6) Rule on motions and other procedural matters;

(7) Regulate the scope and timing of documentary discovery as permitted by this subpart;

(8) Regulate the course of the hearing and the conduct of representatives, parties, and witnesses;

(9) Examine witnesses;

(10) Receive, rule on, exclude, or limit evidence;

(11) Upon motion of a party, take official notice of facts;

(12) Conduct any conference, argument or hearing in person or, upon agreement of the parties, by telephone; and

(13) Upon motion of a party, decide cases, in whole or in part, by summary judgment where there is no disputed issue of material fact. A summary judgment decision constitutes a hearing on the record for the purposes of this subpart.

(c) The ALJ—

(1) May not find invalid or refuse to follow Federal statutes, regulations, or Secretarial delegations of authority and must give deference to published guidance to the extent not inconsistent with statute or regulation;

(2) May not enter an order in the nature of a directed verdict;

(3) May not compel settlement negotiations;

(4) May not enjoin any act of the Secretary; or

(5) May not review the exercise of discretion by the Secretary with respect to whether to grant an extension under § 160.410(b)(2)(ii)(B) or (c)(2)(ii) of this part or to provide technical assistance under 42 U.S.C. 1320d-5(b)(2)(B).

§ 160.510 Ex parte contacts.

No party or person (except employees of the ALJ's office) may communicate in any way with the ALJ on any matter at issue in a case, unless on notice and opportunity for both parties to participate. This provision does not prohibit a party or person from inquiring about the status of a case or asking routine questions concerning administrative functions or procedures.

§ 160.512 Prehearing conferences.

(a) The ALJ must schedule at least one prehearing conference, and may schedule additional prehearing conferences as appropriate, upon reasonable notice, which may not be less than 14 business days, to the parties.

(b) The ALJ may use prehearing conferences to discuss the following—

(1) Simplification of the issues;

(2) The necessity or desirability of amendments to the pleadings, including the need for a more definite statement;

(3) Stipulations and admissions of fact or as to the contents and authenticity of documents;

(4) Whether the parties can agree to submission of the case on a stipulated record;

(5) Whether a party chooses to waive appearance at an oral hearing and to submit only documentary evidence (subject to the objection of the other party) and written argument;

(6) Limitation of the number of witnesses;

(7) Scheduling dates for the exchange of witness lists and of proposed exhibits;

(8) Discovery of documents as permitted by this subpart;

(9) The time and place for the hearing;

(10) The potential for the settlement of the case by the parties; and

(11) Other matters as may tend to encourage the fair, just and expeditious disposition of the proceedings, including the protection of privacy of individually identifiable health information that may be submitted into evidence or otherwise used in the proceeding, if appropriate.

(c) The ALJ must issue an order containing the matters agreed upon by the parties or ordered by the ALJ at a prehearing conference.

§ 160.514 Authority to settle.

The Secretary has exclusive authority to settle any issue or case without the consent of the ALJ.

§ 160.516 Discovery.

(a) A party may make a request to another party for production of documents for inspection and copying that are relevant and material to the issues before the ALJ.

(b) For the purpose of this section, the term "documents" includes information, reports, answers, records, accounts, papers and other data and documentary evidence. Nothing contained in this section may be interpreted to require the creation of a document, except that requested data stored in an electronic data storage system must be produced in a form accessible to the requesting party.

(c) Requests for documents, requests for admissions, written interrogatories, depositions and any forms of discovery, other than those permitted under paragraph (a) of this section, are not authorized.

(d) This section may not be construed to require the disclosure of interview reports or statements obtained by any party, or on behalf of any party, of persons who will not be called as witnesses by that party, or analyses and summaries prepared in conjunction with the investigation or litigation of the case, or any otherwise privileged documents.

(e)(1) When a request for production of documents has

been received, within 30 days the party receiving that request must either fully respond to the request, or state that the request is being objected to and the reasons for that objection. If objection is made to part of an item or category, the part must be specified. Upon receiving any objections, the party seeking production may then, within 30 days or any other time frame set by the ALJ, file a motion for an order compelling discovery. The party receiving a request for production may also file a motion for protective order any time before the date the production is due.

(2) The ALJ may grant a motion for protective order or deny a motion for an order compelling discovery if the ALJ finds that the discovery sought—

(i) Is irrelevant;

(ii) Is unduly costly or burdensome;

(iii) Will unduly delay the proceeding; or

(iv) Seeks privileged information.

(3) The ALJ may extend any of the time frames set forth in paragraph (e)(1) of this section.

(4) The burden of showing that discovery should be allowed is on the party seeking discovery.

§ 160.518 Exchange of witness lists, witness statements, and exhibits.

(a) The parties must exchange witness lists, copies of prior written statements of proposed witnesses, and copies of proposed hearing exhibits, including copies of any written statements that the party intends to offer in lieu of live testimony in accordance with § 160.538, not more than 60, and not less than 15, days before the scheduled hearing, except that if a respondent intends to introduce the evidence of a statistical expert, the respondent must provide the Secretarial party with a copy of the statistical expert's report not less than 30 days before the scheduled hearing.

(b)(1) If, at any time, a party objects to the proposed admission of evidence not exchanged in accordance with paragraph (a) of this section, the ALJ must determine whether the failure to comply with paragraph (a) of this section should result in the exclusion of that evidence.

(2) Unless the ALJ finds that extraordinary circumstances justified the failure timely to exchange the information listed under paragraph (a) of this section, the ALJ must exclude from the party's case-in-chief—

(i) The testimony of any witness whose name does not appear on the witness list; and

(ii) Any exhibit not provided to the opposing party as specified in paragraph (a) of this section.

(3) If the ALJ finds that extraordinary circumstances existed, the ALJ must then determine whether the admission of that evidence would cause substantial prejudice to the objecting party.

(i) If the ALJ finds that there is no substantial prejudice, the evidence may be admitted.

(ii) If the ALJ finds that there is substantial prejudice, the ALJ may exclude the evidence, or, if he or she does not exclude the evidence, must postpone the hearing for such time as is necessary for the objecting party to prepare and respond to the evidence, unless the objecting party waives postponement.

(c) Unless the other party objects within a reasonable period of time before the hearing, documents exchanged in accordance with paragraph (a) of this section will be deemed to be authentic for the purpose of admissibility at the hearing.

§ 160.520 Subpoenas for attendance at hearing.

(a) A party wishing to procure the appearance and testimony of any person at the hearing may make a motion requesting the ALJ to issue a subpoena if the appearance and testimony are reasonably necessary for the presentation of a party's case.

(b) A subpoena requiring the attendance of a person in accordance with paragraph (a) of this section may also require the person (whether or not the person is a party) to produce relevant and material evidence at or before the hearing.

(c) When a subpoena is served by a respondent on a particular employee or official or particular office of HHS, the Secretary may comply by designating any knowledgeable HHS representative to appear and testify.

(d) A party seeking a subpoena must file a written motion not less than 30 days before the date fixed for the hearing, unless otherwise allowed by the ALJ

for good cause shown. That motion must—

(1) Specify any evidence to be produced;

(2) Designate the witnesses; and

(3) Describe the address and location with sufficient particularity to permit those witnesses to be found.

(e) The subpoena must specify the time and place at which the witness is to appear and any evidence the witness is to produce.

(f) Within 15 days after the written motion requesting issuance of a subpoena is served, any party may file an opposition or other response.

(g) If the motion requesting issuance of a subpoena is granted, the party seeking the subpoena must serve it by delivery to the person named, or by certified mail addressed to that person at the person's last dwelling place or principal place of business.

(h) The person to whom the subpoena is directed may file with the ALJ a motion to quash the subpoena within 10 days after service.

(i) The exclusive remedy for contumacy by, or refusal to obey a subpoena duly served upon, any person is specified in 42 U.S.C. 405(e).

§ 160.522 Fees.

The party requesting a subpoena must pay the cost of the fees and mileage of any witness subpoenaed in the amounts that would be payable to a witness in a proceeding in United States District Court. A check for witness fees and mileage must accompany the subpoena when served, except that, when a subpoena is issued on behalf of the Secretary, a check for witness fees and mileage need not accompany the subpoena.

§ 160.524 Form, filing, and service of papers.

(a) *Forms.* (1) Unless the ALJ directs the parties to do otherwise, documents filed with the ALJ must include an original and two copies.

(2) Every pleading and paper filed in the proceeding must contain a caption setting forth the title of the action, the case number, and a designation of the paper, such as motion to quash subpoena.

(3) Every pleading and paper must be signed by and must contain the address and telephone number of the party or the person on whose behalf the paper was filed, or his or her representative.

(4) Papers are considered filed when they are mailed.

(b) *Service.* A party filing a document with the ALJ or the Board must, at the time of filing, serve a copy of the document on the other party. Service upon any party of any document must be made by delivering a copy, or placing a copy of the document in the United States mail, postage prepaid and addressed, or with a private delivery service, to the party's last known address. When a party is represented by an attorney, service must be made upon the attorney in lieu of the party.

(c) *Proof of service.* A certificate of the natural person serving the document by personal delivery or by mail, setting forth the manner of service, constitutes proof of service.

§ 160.526 Computation of time.

(a) In computing any period of time under this subpart or in an order issued thereunder, the time begins with the day following the act, event or default, and includes the last day of the period unless it is a Saturday, Sunday, or legal holiday observed by the Federal Government, in which event it includes the next business day.

(b) When the period of time allowed is less than 7 days, intermediate Saturdays, Sundays, and legal holidays observed by the Federal Government must be excluded from the computation.

(c) Where a document has been served or issued by placing it in the mail, an additional 5 days must be added to the time permitted for any response. This paragraph does not apply to requests for hearing under § 160.504.

§ 160.528 Motions.

(a) An application to the ALJ for an order or ruling must be by motion. Motions must state the relief sought, the authority relied upon and the facts alleged, and must be filed with the ALJ and served on all other parties.

(b) Except for motions made during a prehearing conference or at the hearing, all motions must be in writing. The ALJ

may require that oral motions be reduced to writing.

(c) Within 10 days after a written motion is served, or such other time as may be fixed by the ALJ, any party may file a response to the motion.

(d) The ALJ may not grant a written motion before the time for filing responses has expired, except upon consent of the parties or following a hearing on the motion, but may overrule or deny the motion without awaiting a response.

(e) The ALJ must make a reasonable effort to dispose of all outstanding motions before the beginning of the hearing.

§ 160.530 Sanctions.

The ALJ may sanction a person, including any party or attorney, for failing to comply with an order or procedure, for failing to defend an action or for other misconduct that interferes with the speedy, orderly or fair conduct of the hearing. The sanctions must reasonably relate to the severity and nature of the failure or misconduct. The sanctions may include—

(a) In the case of refusal to provide or permit discovery under the terms of this part, drawing negative factual inferences or treating the refusal as an admission by deeming the matter, or certain facts, to be established;

(b) Prohibiting a party from introducing certain evidence or otherwise supporting a particular claim or defense;

(c) Striking pleadings, in whole or in part;

(d) Staying the proceedings;

(e) Dismissal of the action;

(f) Entering a decision by default;

(g) Ordering the party or attorney to pay the attorney's fees and other costs caused by the failure or misconduct; and

(h) Refusing to consider any motion or other action that is not filed in a timely manner.

§ 160.532 Collateral estoppel.

When a final determination that the respondent violated an administrative simplification provision has been rendered in any proceeding in which the respondent was a party and had an opportunity to be heard, the respondent is bound by that determination in any proceeding under this part.

§ 160.534 The hearing.

(a) The ALJ must conduct a hearing on the record in order to determine whether the respondent should be found liable under this part.

(b) (1) The respondent has the burden of going forward and the burden of persuasion with respect to any:

(i) Affirmative defense pursuant to § 160.410 of this part;

(ii) Challenge to the amount of a proposed penalty pursuant to §§ 160.404-160.408 of this part, including any factors raised as mitigating factors; or

(iii) Claim that a proposed penalty should be reduced or waived pursuant to § 160.412 of this part; and

(iv) Compliance with subpart D of part 164, as provided under § 164.414(b).

(2) The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed penalty.

(3) The burden of persuasion will be judged by a preponderance of the evidence.

(c) The hearing must be open to the public unless otherwise ordered by the ALJ for good cause shown.

(d)(1) Subject to the 15-day rule under § 160.518(a) and the admissibility of evidence under § 160.540, either party may introduce, during its case in chief, items or information that arose or became known after the date of the issuance of the notice of proposed determination or the request for hearing, as applicable. Such items and information may not be admitted into evidence, if introduced—

(i) By the Secretary, unless they are material and relevant to the acts or omissions with respect to which the penalty is proposed in the notice of proposed determination pursuant to § 160.420 of this part, including circumstances that may increase penalties; or

(ii) By the respondent, unless they are material and relevant to an admission, denial or

explanation of a finding of fact in the notice of proposed determination under § 160.420 of this part, or to a specific circumstance or argument expressly stated in the request for hearing under § 160.504, including circumstances that may reduce penalties.

(2) After both parties have presented their cases, evidence may be admitted in rebuttal even if not previously exchanged in accordance with § 160.518.

[71 FR 8428, Feb. 16, 2006, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5692, Jan. 25, 2013]

§ 160.536 Statistical sampling.

(a) In meeting the burden of proof set forth in § 160.534, the Secretary may introduce the results of a statistical sampling study as evidence of the number of violations under § 160.406 of this part, or the factors considered in determining the amount of the civil money penalty under § 160.408 of this part. Such statistical sampling study, if based upon an appropriate sampling and computed by valid statistical methods, constitutes prima facie evidence of the number of violations and the existence of factors material to the proposed civil money penalty as described in §§ 160.406 and 160.408.

(b) Once the Secretary has made a prima facie case, as described in paragraph (a) of this section, the burden of going forward shifts to the respondent to produce evidence reasonably calculated to rebut the findings of the statistical sampling study. The Secretary will then be given the opportunity to rebut this evidence.

§ 160.538 Witnesses.

(a) Except as provided in paragraph (b) of this section, testimony at the hearing must be given orally by witnesses under oath or affirmation.

(b) At the discretion of the ALJ, testimony of witnesses other than the testimony of expert witnesses may be admitted in the form of a written statement. The ALJ may, at his or her discretion, admit prior sworn testimony of experts that has been subject to adverse examination, such as a deposition or trial testimony. Any such written statement must be provided to the other party, along with the last known address of the witness, in a manner that allows sufficient time for the other party to subpoena the witness for cross-examination at the hearing. Prior written statements of witnesses proposed to testify at the hearing must be exchanged as provided in § 160.518.

(c) The ALJ must exercise reasonable control over the mode and order of interrogating witnesses and presenting evidence so as to:

(1) Make the interrogation and presentation effective for the ascertainment of the truth;

(2) Avoid repetition or needless consumption of time; and

(3) Protect witnesses from harassment or undue embarrassment.

(d) The ALJ must permit the parties to conduct cross-examination of witnesses as may be required for a full and true disclosure of the facts.

(e) The ALJ may order witnesses excluded so that they cannot hear the testimony of other witnesses, except that the ALJ may not order to be excluded—

(1) A party who is a natural person;

(2) In the case of a party that is not a natural person, the officer or employee of the party appearing for the entity pro se or designated as the party's representative; or

(3) A natural person whose presence is shown by a party to be essential to the presentation of its case, including a person engaged in assisting the attorney for the Secretary.

§ 160.540 Evidence.

(a) The ALJ must determine the admissibility of evidence.

(b) Except as provided in this subpart, the ALJ is not bound by the Federal Rules of Evidence. However, the ALJ may apply the Federal Rules of Evidence where appropriate, for example, to exclude unreliable evidence.

(c) The ALJ must exclude irrelevant or immaterial evidence.

(d) Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or by considerations of undue delay or needless presentation of cumulative evidence.

(e) Although relevant, evidence must be excluded if it is privileged under Federal law.

(f) Evidence concerning offers of compromise or settlement are inadmissible to the extent provided in Rule 408 of the Federal Rules of Evidence.

(g) Evidence of crimes, wrongs, or acts other than those at issue in the instant case is admissible in order to show motive, opportunity, intent, knowledge, preparation, identity, lack of mistake, or existence of a scheme. This evidence is admissible regardless of whether the crimes, wrongs, or acts occurred during the statute of limitations period applicable to the acts or omissions that constitute the basis for liability in the case and regardless of whether they were referenced in the Secretary's notice of proposed determination under § 160.420 of this part.

(h) The ALJ must permit the parties to introduce rebuttal witnesses and evidence.

(i) All documents and other evidence offered or taken for the record must be open to examination by both parties, unless otherwise ordered by the ALJ for good cause shown.

§ 160.542 The record.

(a) The hearing must be recorded and transcribed. Transcripts may be obtained following the hearing from the ALJ. A party that requests a transcript of hearing proceedings must pay the cost of preparing the transcript unless, for good cause shown by the party, the payment is waived by the ALJ or the Board, as appropriate.

(b) The transcript of the testimony, exhibits, and other evidence admitted at the hearing, and all papers and requests filed in the proceeding constitute the record for decision by the ALJ and the Secretary.

(c) The record may be inspected and copied (upon payment of a reasonable fee) by any person, unless otherwise ordered by the ALJ for good cause shown.

(d) For good cause, the ALJ may order appropriate redactions made to the record.

§ 160.544 Post hearing briefs.

The ALJ may require the parties to file post-hearing briefs. In any event, any party may file a post-hearing brief. The ALJ must fix the time for filing the briefs. The time for filing may not exceed 60 days from the date the parties receive the transcript of the hearing or, if applicable, the stipulated record. The briefs may be accompanied by proposed findings of fact and conclusions of law. The ALJ may permit the parties to file reply briefs.

§ 160.546 ALJ's decision.

(a) The ALJ must issue a decision, based only on the record, which must contain findings of fact and conclusions of law.

(b) The ALJ may affirm, increase, or reduce the penalties imposed by the Secretary.

(c) The ALJ must issue the decision to both parties within 60 days after the time for submission of post-hearing briefs and reply briefs, if permitted, has expired. If the ALJ fails to meet the deadline contained in this paragraph, he or she must notify the parties of the reason for the delay and set a new deadline.

(d) Unless the decision of the ALJ is timely appealed as provided for in § 160.548, the decision of the ALJ will be final and binding on the parties 60 days from the date of service of the ALJ's decision.

§ 160.548 Appeal of the ALJ's decision.

(a) Any party may appeal the decision of the ALJ to the Board by filing a notice of appeal with the Board within 30 days of the date of service of the ALJ decision. The Board may extend the initial 30 day period for a period of time not to exceed 30 days if a party files with the Board a request for an extension within the initial 30 day period and shows good cause.

(b) If a party files a timely notice of appeal with the Board, the ALJ must forward the record of the proceeding to the Board.

(c) A notice of appeal must be accompanied by a written brief specifying exceptions to the initial decision and reasons supporting the exceptions. Any party may file a brief in opposition to the exceptions, which may raise any relevant issue not addressed in the exceptions, within 30 days of receiving the notice of appeal and the accompanying brief. The Board may permit the parties to file reply briefs.

(d) There is no right to appear personally before the Board or to appeal to the Board any interlocutory ruling by the ALJ.

(e) Except for an affirmative defense under § 160.410(a)(1) or (2) of this part, the Board may not consider any issue not raised in the parties' briefs, nor any issue in the briefs that could have been raised before the ALJ but was not.

(f) If any party demonstrates to the satisfaction of the Board that additional evidence not presented at such hearing is relevant and material and that there were reasonable grounds for the failure to adduce such evidence at the hearing, the Board may remand the matter to the ALJ for consideration of such additional evidence.

(g) The Board may decline to review the case, or may affirm, increase, reduce, reverse or remand any penalty determined by the ALJ.

(h) The standard of review on a disputed issue of fact is whether the initial decision of the ALJ is supported by substantial evidence on the whole record. The standard of review on a disputed issue of law is whether the decision is erroneous.

(i) Within 60 days after the time for submission of briefs and reply briefs, if permitted, has expired, the Board must serve on each party to the appeal a copy of the Board's decision and a statement describing the right of any respondent who is penalized to seek judicial review.

(j)(1) The Board's decision under paragraph (i) of this section, including a decision to decline review of the initial decision, becomes the final decision of the Secretary 60 days after the date of service of the Board's decision, except with respect to a decision to remand to the ALJ or if reconsideration is requested under this paragraph.

(2) The Board will reconsider its decision only if it determines that the decision contains a clear error of fact or error of law. New evidence will not be a basis for reconsideration unless the party demonstrates that the evidence is newly discovered and was not previously available.

(3) A party may file a motion for reconsideration with the Board before the date the decision becomes final under paragraph (j)(1) of this section. A motion for reconsideration must be accompanied by a written brief specifying any alleged error of fact or law and, if the party is relying on additional evidence, explaining why the evidence was not previously available. Any party may file a brief in opposition within 15 days of receiving the motion for reconsideration and the accompanying brief unless this time limit is extended by the Board for good cause shown. Reply briefs are not permitted.

(4) The Board must rule on the motion for reconsideration not later than 30 days from the date the opposition brief is due. If the Board denies the motion, the decision issued under paragraph (i) of this section becomes the final decision of the Secretary on the date of service of the ruling. If the Board grants the motion, the Board will issue a reconsidered decision, after such procedures as the Board determines necessary to address the effect of any error. The Board's decision on reconsideration becomes the final decision of the Secretary on the date of service of the decision, except with respect to a decision to remand to the ALJ.

(5) If service of a ruling or decision issued under this section is by mail, the date of service will be deemed to be 5 days from the date of mailing.

(k)(1) A respondent's petition for judicial review must be filed within 60 days of the date on which the decision of the Board becomes the final decision of the Secretary under paragraph (j) of this section.

(2) In compliance with 28 U.S.C. 2112(a), a copy of any petition for judicial review filed in any U.S. Court of Appeals challenging the final decision of the Secretary must be sent by certified mail, return receipt requested, to the General Counsel of HHS. The petition copy must be a copy showing that it has been time-stamped by the clerk of the court when the original was filed with the court.

(3) If the General Counsel of HHS received two or more petitions within 10 days after the final decision of the Secretary, the General Counsel will notify the U.S. Judicial Panel on Multidistrict Litigation of any petitions that were received within the 10 day period.

§ 160.550 Stay of the Secretary's decision.

(a) Pending judicial review, the respondent may file a request for stay of the effective date of any penalty with the ALJ. The request must be accompanied by a copy of the notice of appeal filed with the Federal court. The filing of the request automatically stays the effective date of the penalty until such

time as the ALJ rules upon the request.

(b) The ALJ may not grant a respondent's request for stay of any penalty unless the respondent posts a bond or provides other adequate security.

(c) The ALJ must rule upon a respondent's request for stay within 10 days of receipt.

§ 160.552 Harmless error.

No error in either the admission or the exclusion of evidence, and no error or defect in any ruling or order or in any act done or omitted by the ALJ or by any of the parties is ground for vacating, modifying or otherwise disturbing an otherwise appropriate ruling or order or act, unless refusal to take such action appears to the ALJ or the Board inconsistent with substantial justice. The ALJ and the Board at every stage of the proceeding must disregard any error or defect in the proceeding that does not affect the substantial rights of the parties.

PART 162—ADMINISTRATIVE REQUIREMENTS

Contents

Subpart A—General Provisions

§ 162.100 Applicability.
§ 162.103 Definitions.

Subparts B-C [Reserved]

Subpart D—Standard Unique Health Identifier for Health Care Providers

§ 162.402 [Reserved]
§ 162.404 Compliance dates of the implementation of the standard unique health identifier for health care providers.
§ 162.406 Standard unique health identifier for health care providers.
§ 162.408 National Provider System.
§ 162.410 Implementation specifications: Health care providers.
§ 162.412 Implementation specifications: Health plans.
§ 162.414 Implementation specifications: Health care clearinghouses.

Subpart E—Standard Unique Health Identifier for Health Plans

§ 162.502 [Reserved]
§ 162.504 Compliance requirements for the implementation of the standard unique health plan identifier.
§ 162.506 Standard unique health plan identifier.
§ 162.508 Enumeration System.
§ 162.510 Full implementation requirements: Covered entities.
§ 162.512 Implementation specifications: Health plans.
§ 162.514 Other entity identifier.

Subpart F—Standard Unique Employer Identifier

§ 162.600 Compliance dates of the implementation of the standard unique employer identifier.
§ 162.605 Standard unique employer identifier.
§ 162.610 Implementation specifications for covered entities.

Subparts G-H [Reserved]

Subpart I—General Provisions for Transactions

§ 162.900 [Reserved]
§ 162.910 Maintenance of standards and adoption of modifications and new standards.
§ 162.915 Trading partner agreements.
§ 162.920 Availability of implementation specifications and operating rules.
§ 162.923 Requirements for covered entities.
§ 162.925 Additional requirements for health plans.
§ 162.930 Additional rules for health care clearinghouses.
§ 162.940 Exceptions from standards to permit testing of proposed modifications.

Subpart J—Code Sets

§ 162.1000 General requirements.
§ 162.1002 Medical data code sets.
§ 162.1011 Valid code sets.

Subpart K—Health Care Claims or Equivalent Encounter Information

§ 162.1101 Health care claims or equivalent encounter information transaction.
§ 162.1102 Standards for health care claims or equivalent encounter information transaction.

Subpart L—Eligibility for a Health Plan

§ 162.1201 Eligibility for a health plan transaction.
§ 162.1202 Standards for eligibility for a health plan transaction.
§ 162.1203 Operating rules for eligibility for a health plan transaction.

Subpart M—Referral Certification and Authorization

§ 162.1301 Referral certification and authorization transaction.
§ 162.1302 Standards for referral certification and authorization transaction.

Subpart N—Health Care Claim Status

§ 162.1401 Health care claim status transaction.
§ 162.1402 Standards for health care claim status transaction.
§ 162.1403 Operating rules for health care claim status transaction.

Subpart O—Enrollment and Disenrollment in a Health Plan

§ 162.1501 Enrollment and disenrollment in a health plan transaction.
§ 162.1502 Standards for enrollment and disenrollment in a health plan transaction.

Subpart P—Health Care Electronic Funds Transfers (EFT) and Remittance Advice

§ 162.1601 Health care electronic funds transfers (EFT) and remittance advice transaction.
§ 162.1602 Standards for health care electronic funds transfers (EFT) and remittance advice transaction.
§ 162.1603 Operating rules for health care electronic funds transfers (EFT) and remittance advice transaction.

Subpart Q—Health Plan Premium Payments

§ 162.1701 Health plan premium payments transaction.
§ 162.1702 Standards for health plan premium payments transaction.

Subpart R—Coordination of Benefits

§ 162.1801 Coordination of benefits transaction.
§ 162.1802 Standards for coordination of benefits information transaction.

Subpart S—Medicaid Pharmacy Subrogation

§ 162.1901 Medicaid pharmacy subrogation transaction.
§ 162.1902 Standard for Medicaid pharmacy subrogation transaction.

AUTHORITY: Secs. 1171 through 1180 of the Social Security Act (42 U.S.C. 1320d-1320d-9), as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031, sec. 105 of Pub. L. 110-233, 122 Stat. 881-922, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note), and secs. 1104 and 10109 of Pub. L. 111-148, 124 Stat. 146-154 and 915-917.

SOURCE: 65 FR 50367, Aug. 17, 2000, unless otherwise noted.

Subpart A—General Provisions

§ 162.100 Applicability.

Covered entities (as defined in § 160.103 of this subchapter) must comply with the applicable requirements of this part.

§ 162.103 Definitions.

For purposes of this part, the following definitions apply:

Code set means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes.

Code set maintaining organization means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part.

Controlling health plan (CHP) means a health plan that—

(1) Controls its own business activities, actions, or policies; or

(2)(i) Is controlled by an entity that is not a health plan; and

(ii) If it has a subhealth plan(s) (as defined in this section), exercises sufficient control over the subhealth plan(s) to direct its/their business activities, actions, or policies.

Covered health care provider means a health care provider that meets the definition at paragraph (3) of the definition of "covered entity" at § 160.103.

Data condition means the rule that describes the circumstances under which a covered entity must use a particular data element or segment.

Data content means all the data elements and code sets inherent to a transaction, and not related to the format of the transaction. Data elements that are related to the format are not data content.

Data element means the smallest named unit of information in a transaction.

Data set means a semantically meaningful unit of information exchanged between two parties to a transaction.

Descriptor means the text defining a code.

Designated standard maintenance organization (DSMO) means an organization designated by the Secretary under § 162.910(a).

Direct data entry means the direct entry of data (for example, using dumb terminals or web browsers) that is immediately transmitted into a health plan's computer.

Format refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction.

HCPCS stands for the Health [Care Financing Administration] Common Procedure Coding System.

Maintain or *maintenance* refers to activities necessary to support the use of a standard adopted by the Secretary, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification.

Maximum defined data set means all of the required data elements for a particular standard based on a specific implementation specification.

Operating rules means the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications as adopted for purposes of this part.

Segment means a group of related data elements in a transaction.

Stage 1 payment initiation means a health plan's order, instruction or authorization to its financial institution to make a health care claims payment using an electronic funds transfer (EFT) through the ACH Network.

Standard transaction means a transaction that complies with an applicable standard and associated operating rules adopted under this part.

Subhealth plan (SHP) means a health plan whose business activities, actions, or policies are directed by a controlling health plan.

[65 FR 50367, Aug. 17, 2000, as amended at 68 FR 8374, Feb. 20, 2003; 74 FR 3324, Jan. 16, 2009; 76 FR 40495, July 8, 2011; 77 FR 1589, Jan. 10, 2012; 77 FR 54719, Sept. 5, 2012]

Subparts B-C [Reserved]

Subpart D—Standard Unique Health Identifier for Health Care Providers

SOURCE: 69 FR 3468, Jan. 23, 2004, unless otherwise noted.

§ 162.402 [Reserved]

§ 162.404 Compliance dates of the implementation of the standard unique health identifier for health care providers.

(a) *Health care providers.* A covered health care provider must comply with the implementation specifications in § 162.410 no later than May 23, 2007.

(b) *Health plans.* A health plan must comply with the implementation specifications in § 162.412 no later than one of the following dates:

(1) A health plan that is not a small health plan—May 23, 2007.

(2) A small health plan—May 23, 2008.

(c) *Health care clearinghouses.* A health care clearinghouse must comply with the implementation specifications in § 162.414 no later than May 23, 2007.

[69 FR 3468, Jan. 23, 2004, as amended at 77 FR 54719, Sept. 5, 2012]

§ 162.406 Standard unique health identifier for health care providers.

(a) *Standard.* The standard unique health identifier for health care providers is the National Provider Identifier (NPI). The NPI is a 10-position numeric identifier, with a check digit in the 10th position, and no intelligence about the health care provider in the number.

(b) *Required and permitted uses for the NPI.* (1) The NPI must be used as stated in § 162.410, § 162.412, and § 162.414.

(2) The NPI may be used for any other lawful purpose.

§ 162.408 National Provider System.

National Provider System. The National Provider System (NPS) shall do the following:

(a) Assign a single, unique NPI to a health care provider, provided that—

(1) The NPS may assign an NPI to a subpart of a health care provider in accordance with paragraph (g); and

(2) The Secretary has sufficient information to permit the assignment to be made.

(b) Collect and maintain information about each health

care provider that has been assigned an NPI and perform tasks necessary to update that information.

(c) If appropriate, deactivate an NPI upon receipt of appropriate information concerning the dissolution of the health care provider that is an organization, the death of the health care provider who is an individual, or other circumstances justifying deactivation.

(d) If appropriate, reactivate a deactivated NPI upon receipt of appropriate information.

(e) Not assign a deactivated NPI to any other health care provider.

(f) Disseminate NPS information upon approved requests.

(g) Assign an NPI to a subpart of a health care provider on request if the identifying data for the subpart are unique.

§ 162.410 Implementation specifications: Health care providers.

(a) A covered entity that is a covered health care provider must:

(1) Obtain, by application if necessary, an NPI from the National Provider System (NPS) for itself or for any subpart of the covered entity that would be a covered health care provider if it were a separate legal entity. A covered entity may obtain an NPI for any other subpart that qualifies for the assignment of an NPI.

(2) Use the NPI it obtained from the NPS to identify itself on all standard transactions that it conducts where its health care provider identifier is required.

(3) Disclose its NPI, when requested, to any entity that needs the NPI to identify that covered health care provider in a standard transaction.

(4) Communicate to the NPS any changes in its required data elements in the NPS within 30 days of the change.

(5) If it uses one or more business associates to conduct standard transactions on its behalf, require its business associate(s) to use its NPI and other NPIs appropriately as required by the transactions that the business associate(s) conducts on its behalf.

(6) If it has been assigned NPIs for one or more subparts, comply with the requirements of paragraphs (a)(2) through (a)(5) of this section with respect to each of those NPIs.

(b) An organization covered health care provider that has as a member, employs, or contracts with, an individual health care provider who is not a covered entity and is a prescriber, must require such health care provider to—

(1) Obtain an NPI from the National Plan and Provider Enumeration System (NPPES); and

(2) To the extent the prescriber writes a prescription while acting within the scope of the prescriber's relationship with the organization, disclose the NPI upon request to any entity that needs it to identify the prescriber in a standard transaction.

(c) A health care provider that is not a covered entity may obtain, by application if necessary, an NPI from the NPS.

[69 FR 3468, Jan. 23, 2004, as amended at 77 FR 54719, Sept. 5, 2012]

§ 162.412 Implementation specifications: Health plans.

(a) A health plan must use the NPI of any health care provider (or subpart(s), if applicable) that has been assigned an NPI to identify that health care provider on all standard transactions where that health care provider's identifier is required.

(b) A health plan may not require a health care provider that has been assigned an NPI to obtain an additional NPI.

§ 162.414 Implementation specifications: Health care clearinghouses.

A health care clearinghouse must use the NPI of any health care provider (or subpart(s), if applicable) that has been assigned an NPI to identify that health care provider on all standard transactions where that health care provider's identifier is required.

Subpart E—Standard Unique Health Identifier for Health Plans

SOURCE: 77 FR 54719, Sept. 5, 2012, unless otherwise noted.

§ 162.502 [Reserved]

§ 162.504 Compliance requirements for the implementation of the standard unique health plan identifier.

(a) *Covered entities.* A covered entity must comply with the implementation requirements in § 162.510 no later than November 7, 2016.

(b) *Health plans.* A health plan must comply with the implementation specifications in § 162.512 no later than one of the following dates:

(1) A health plan that is not a small health plan— November 5, 2014.

(2) A health plan that is a small health plan— November 5, 2015.

[77 FR 54719, Sept. 5, 2012, as amended at 77 FR 60630, Oct. 4, 2012]

§ 162.506 Standard unique health plan identifier.

(a) *Standard.* The standard unique health plan identifier is the Health Plan Identifier (HPID) that is assigned by the Enumeration System identified in § 162.508.

(b) *Required and permitted uses for the HPID.* (1) The HPID must be used as specified in § 162.510 and § 162.512.

(2) The HPID may be used for any other lawful purpose.

§ 162.508 Enumeration System.

The Enumeration System must do all of the following:

(a) Assign a single, unique—

(1) HPID to a health plan, provided that the Secretary has sufficient information to permit the assignment to be made; or

(2) OEID to an entity eligible to receive one under § 162.514(a), provided that the Secretary has sufficient information to permit the assignment to be made.

(b) Collect and maintain information about each health plan that applies for or has been assigned an HPID and each entity that applies for or has been assigned an OEID, and perform tasks necessary to update that information.

(c) If appropriate, deactivate an HPID or OEID upon receipt of sufficient information concerning circumstances justifying deactivation.

(d) If appropriate, reactivate a deactivated HPID or OEID upon receipt of sufficient information justifying reactivation.

(e) Not assign a deactivated HPID to any other health plan or OEID to any other entity.

(f) Disseminate Enumeration System information upon approved requests.

§ 162.510 Full implementation requirements: Covered entities.

(a) A covered entity must use an HPID to identify a health plan that has an HPID when a covered entity identifies a health plan in a transaction for which the Secretary has adopted a standard under this part.

(b) If a covered entity uses one or more business associates to conduct standard transactions on its behalf, it must require its business associate(s) to use an HPID to identify a health plan that has an HPID when the business associate(s) identifies a health plan in a transaction for which the Secretary has adopted a standard under this part.

§ 162.512 Implementation specifications: Health plans.

(a) A controlling health plan must do all of the following:

(1) Obtain an HPID from the Enumeration System for itself.

(2) Disclose its HPID, when requested, to any entity that needs the HPID to identify the health plan in a standard transaction.

(3) Communicate to the Enumeration System any changes in its required data elements in the Enumeration System within 30 days of the change.

(b) A controlling health plan may do the following:

(1) Obtain an HPID from the Enumeration System for a subhealth plan of the controlling health plan.

(2) Direct a subhealth plan of the controlling health plan to obtain an HPID from the Enumeration System.

(c) A subhealth plan may obtain an HPID from the Enumeration System.

(d) A subhealth plan that is assigned an HPID from the Enumeration System must comply with the requirements that apply to a controlling health plan in paragraphs (a)(2) and (a)(3) of this section.

§ 162.514 Other entity identifier.

(a) An entity may obtain an Other Entity Identifier (OEID) to identify itself if the entity meets all of the following:

(1) Needs to be identified in a transaction for which the Secretary has adopted a standard under this part.

(2) Is not eligible to obtain an HPID.

(3) Is not eligible to obtain an NPI.

(4) Is not an individual.

(b) An OEID must be obtained from the Enumeration System identified in § 162.508.

(c) *Uses for the OEID.* (1) An other entity may use the OEID it obtained from the Enumeration System to identify itself or have itself identified on all covered transactions in which it needs to be identified.

(2) The OEID may be used for any other lawful purpose.

Subpart F—Standard Unique Employer Identifier

SOURCE: 67 FR 38020, May 31, 2002, unless otherwise noted.

§ 162.600 Compliance dates of the implementation of the standard unique employer identifier.

(a) *Health care providers.* Health care providers must comply with the requirements of this subpart no later than July 30, 2004.

(b) *Health plans.* A health plan must comply with the requirements of this subpart no later than one of the following dates:

(1) *Health plans other than small health plans* —July 30, 2004.

(2) *Small health plans* —August 1, 2005.

(c) *Health care clearinghouses.* Health care clearinghouses must comply with the requirements of this subpart no later than July 30, 2004.

§ 162.605 Standard unique employer identifier.

The Secretary adopts the EIN as the standard unique employer identifier provided for by 42 U.S.C. 1320d-2(b).

§ 162.610 Implementation specifications for covered entities.

(a) The standard unique employer identifier of an employer of a particular employee is the EIN that appears on that employee's IRS Form W-2, Wage and Tax Statement, from the employer.

(b) A covered entity must use the standard unique employer identifier (EIN) of the appropriate employer in standard transactions that require an employer identifier to identify a person or entity as an employer, including where situationally required.

(c) Required and permitted uses for the Employer Identifier.

(1) The Employer Identifier must be used as stated in § 162.610(b).

(2) The Employer Identifier may be used for any other lawful purpose.

[67 FR 38020, May 31, 2002, as amended at 69 FR 3469, Jan. 23, 2004]

Subparts G-H [Reserved]

Subpart I—General Provisions for Transactions

§ 162.900 [Reserved]

§ 162.910 Maintenance of standards and adoption of modifications and new standards.

(a) *Designation of DSMOs.* (1) The Secretary may designate as a DSMO an organization that agrees to conduct, to the satisfaction of the Secretary, the following functions:

(i) Maintain standards adopted under this subchapter.

(ii) Receive and process requests for adopting a new standard or modifying an adopted standard.

(2) The Secretary designates a DSMO by notice in the FEDERAL REGISTER.

(b) *Maintenance of standards.* Maintenance of a standard by the appropriate DSMO constitutes maintenance of the standard for purposes of this part, if done in accordance with the processes the Secretary may require.

(c) *Process for modification of existing standards and adoption*

of new standards. The Secretary considers a recommendation for a proposed modification to an existing standard, or a proposed new standard, only if the recommendation is developed through a process that provides for the following:

(1) Open public access.

(2) Coordination with other DSMOs.

(3) An appeals process for each of the following, if dissatisfied with the decision on the request:

(i) The requestor of the proposed modification.

(ii) A DSMO that participated in the review and analysis of the request for the proposed modification, or the proposed new standard.

(4) Expedited process to address content needs identified within the industry, if appropriate.

(5) Submission of the recommendation to the National Committee on Vital and Health Statistics (NCVHS).

§ 162.915 Trading partner agreements.

A covered entity must not enter into a trading partner agreement that would do any of the following:

(a) Change the definition, data condition, or use of a data element or segment in a standard or operating rule, except where necessary to implement State or Federal law, or to protect against fraud and abuse.

(b) Add any data elements or segments to the maximum defined data set.

(c) Use any code or data elements that are either marked "not used" in the standard's implementation specification or are not in the standard's implementation specification(s).

(d) Change the meaning or intent of the standard's implementation specification(s).

[65 FR 50367, Aug. 17, 2000, as amended at 76 FR 40495, July 8, 2011]

§ 162.920 Availability of implementation specifications and operating rules.

Certain material is incorporated by reference into this subpart with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in this section, the Department of Health and Human Services must publish notice of change in the FEDERAL REGISTER and the material must be available to the public. All approved material is available for inspection at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call (202) 714-6030, or go to: *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html.* The materials are also available for inspection by the public at the Centers for Medicare & Medicaid Services (CMS), 7500 Security Boulevard, Baltimore, Maryland 21244. For more information on the availability on the materials at CMS, call (410) 786-6597. The materials are also available from the sources listed below.

(a) *ASC X12N specifications and the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3.* The implementation specifications for the ASC X12N and the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 (and accompanying Errata or Type 1 Errata) may be obtained from the ASC X12, 7600 Leesburg Pike, Suite 430, Falls Church, VA 22043; Telephone (703) 970-4480; and FAX (703) 970-4488. They are also available through the internet at *http://www.X12.org*. A fee is charged for all implementation specifications, including Technical Reports Type 3. Charging for such publications is consistent with the policies of other publishers of standards. The transaction implementation specifications are as follows:

(1) The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097 and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1, as referenced in § 162.1102 and § 162.1802.

(2) The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claim: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X098A1, as referenced in § 162.1102 and § 162.1802.

(3) The ASC X12N 837—Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096 and Addenda to Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X096A1 as referenced in § 162.1102 and § 162.1802.

(4) The ASC X12N 835—Health Care Claim Payment/Advice, Version 4010, May 2000, Washington Publishing Company, 004010X091, and Addenda to Health Care Claim Payment/Advice, Version 4010, October 2002, Washington Publishing Company, 004010X091A1 as referenced in § 162.1602.

(5) ASC X12N 834—Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095 and Addenda to Benefit Enrollment and Maintenance, Version 4010, October 2002, Washington Publishing Company, 004010X095A1, as referenced in § 162.1502.

(6) The ASC X12N 820—Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061, and Addenda to Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, October 2002, Washington Publishing Company, 004010X061A1, as referenced in § 162.1702.

(7) The ASC X12N 278—Health Care Services Review—Request for Review and Response, Version 4010, May 2000, Washington Publishing Company, 004010X094 and Addenda to Health Care Services Review—Request for Review and Response, Version 4010, October 2002, Washington Publishing Company, 004010X094A1, as referenced in § 162.1302.

(8) The ASC X12N-276/277 Health Care Claim Status Request and Response, Version 4010, May 2000, Washington Publishing Company, 004010X093 and Addenda to Health Care Claim Status Request and Response, Version 4010, October 2002, Washington Publishing Company, 004010X093A1, as referenced in § 162.1402.

(9) The ASC X12N 270/271—Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092 and Addenda to Health Care Eligibility Benefit Inquiry and Response, Version 4010, October 2002, Washington Publishing Company, 004010X092A1, as referenced in § 162.1202.

(10) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006, ASC X12N/005010X224, and Type 1 Errata to Health Care Claim Dental (837), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X224A1, as referenced in § 162.1102 and § 162.1802.

(11) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12, 005010X222, as referenced in § 162.1102 and § 162.1802.

(12) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12/N005010X223, and Type 1 Errata to Health Care Claim: Institutional (837), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1, as referenced in § 162.1102 and § 162.1802.

(13) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221, as referenced in § 162.1602.

(14) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Benefit Enrollment and Maintenance (834), August 2006, ASC X12N/005010X220, as referenced in § 162.1502.

(15) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Payroll Deducted and Other Group Premium Payment for Insurance Products (820), February 2007, ASC X12N/005010X218, as referenced in § 162.1702.

(16) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Services Review—Request for Review and Response (278), May 2006, ASC X12N/005010X217, and Errata to Health Care Services

Review—Request for Review and Response (278), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X217E1, as referenced in § 162.1302.

(17) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Status Request and Response (276/277), August 2006, ASC X12N/005010X212, and Errata to Health Care Claim Status Request and Response (276/277), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X212E1, as referenced in § 162.1402.

(18) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Eligibility Benefit Inquiry and Response (270/271), April 2008, ASC X12N/005010X279, as referenced in § 162.1202.

(b) *Retail pharmacy specifications and Medicaid subrogation implementation guides.* The implementation specifications for the retail pharmacy standards and the implementation specifications for the batch standard for the Medicaid pharmacy subrogation transaction may be obtained from the National Council for Prescription Drug Programs, 9240 East Raintree Drive, Scottsdale, AZ 85260. Telephone (480) 477-1000; FAX (480) 767-1042. They are also available through the Internet at *http://www.ncpdp.org*. A fee is charged for all NCPDP Implementation Guides. Charging for such publications is consistent with the policies of other publishers of standards. The transaction implementation specifications are as follows:

(1) The Telecommunication Standard Implementation Guide Version 5, Release 1 (Version 5.1), September 1999, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, § 162.1602, and § 162.1802.

(2) The Batch Standard Batch Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000, supporting Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, and § 162.1802.

(3) The National Council for Prescription Drug Programs (NCPDP) equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1, Release 0, February 1, 1996, as referenced in § 162.1102, § 162.1202, § 162.1602, and § 162.1802.

(4) The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, and § 162.1802.

(5) The Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), January 2006, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, and § 162.1802.

(6) The Batch Standard Medicaid Subrogation Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007, National Council for Prescription Drug Programs, as referenced in § 162.1902.

(c) Council for Affordable Quality Healthcare's (CAQH) Committee on Operating Rules for Information Exchange (CORE), 601 Pennsylvania Avenue, NW. South Building, Suite 500 Washington, DC 20004; Telephone (202) 861-1492; Fax (202) 861- 1454; E-mail *info@CAQH.org*; and Internet at *http://www.caqh.org/benefits.php*.

(1) CAQH, Committee on Operating Rules for Information Exchange, CORE Phase I Policies and Operating Rules, Approved April 2006, v5010 Update March 2011.

(i) Phase I CORE 152: Eligibility and Benefit Real Time Companion Guide Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(ii) Phase I CORE 153: Eligibility and Benefits Connectivity Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(iii) Phase I CORE 154: Eligibility and Benefits 270/271 Data Content Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(iv) Phase I CORE 155: Eligibility and Benefits Batch Response Time Rule, version

1.1.0, March 2011, as referenced in § 162.1203.

(v) Phase I CORE 156: Eligibility and Benefits Real Time Response Time Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(vi) Phase I CORE 157: Eligibility and Benefits System Availability Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(2) ACME Health Plan, HIPAA Transaction Standard Companion Guide, Refers to the Implementation Guides Based on ASC X12 version 005010, CORE v5010 Master Companion Guide Template, 005010, 1.2, (CORE v 5010 Master Companion Guide Template, 005010, 1.2), March 2011, as referenced in §§ 162.1203, 162.1403, and 162.1603.

(3) CAQH, Committee on Operating Rules for Information Exchange, CORE Phase II Policies and Operating Rules, Approved July 2008, v5010 Update March 2011.

(i) Phase II CORE 250: Claim Status Rule, version 2.1.0, March 2011, as referenced in § 162.1403.

(ii) Phase II CORE 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(iii) Phase II CORE 259: Eligibility and Benefits 270/271 AAA Error Code Reporting Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(iv) Phase II CORE 260: Eligibility & Benefits Data Content (270/271) Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(v) Phase II CORE 270: Connectivity Rule, version 2.2.0, March 2011, as referenced in § 162.1203 and § 162.1403.

(4) Council for Affordable Quality Healthcare (CAQH) Phase III Committee on Operating Rules for Information Exchange (CORE) EFT & ERA Operating Rule Set, Approved June 2012, as specified in this paragraph and referenced in § 162.1603.

(i) Phase III CORE 380 EFT Enrollment Data Rule, version 3.0.0, June 2012.

(ii) Phase III CORE 382 ERA Enrollment Data Rule, version 3.0.0, June 2012.

(iii) Phase III 360 CORE Uniform Use of CARCs and RARCs (835) Rule, version 3.0.0, June 2012.

(iv) CORE-required Code Combinations for CORE-defined Business Scenarios for the Phase III CORE 360 Uniform Use of Claim Adjustment Reason Codes and Remittance Advice Remark Codes (835) Rule, version 3.0.0, June 2012.

(v) Phase III CORE 370 EFT & ERA Reassociation (CCD+/835) Rule, version 3.0.0, June 2012.

(vi) Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012, except Requirement 4.2 titled "Health Care Claim Payment/Advice Batch Acknowledgement Requirements".

(d) The National Automated Clearing House Association (NACHA), The Electronic Payments Association, 1350 Sunrise Valle Drive, Suite 100, Herndon, Virginia 20171 (Phone) (703) 561-1100; (Fax) (703) 713-1641; Email: *info@nacha.org;* and Internet at *http://www.nacha.org.* The implementation specifications are as follows:

(1) 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network, NACHA Operating Rules, Appendix One: ACH File Exchange Specifications (Operating Rule 59) as referenced in § 162.1602.

(2) 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network, NACHA Operating Rules Appendix Three: ACH Record Format Specifications (Operating Rule 78), Part 3.1, Subpart 3.1.8 Sequence of Records for CCD Entries as referenced in § 162.1602.

[68 FR 8396, Feb. 20, 2003, as amended at 69 FR 18803, Apr. 9, 2004; 74 FR 3324, Jan. 16, 2009; 76 FR 40495, July 8, 2011; 77 FR 1590, Jan. 10, 2012; 77 FR 48043, Aug. 10, 2012]

§ 162.923 Requirements for covered entities.

(a) *General rule.* Except as otherwise provided in this part, if a covered entity conducts, with another covered entity that is required to comply with a transaction standard adopted

under this part (or within the same covered entity), using electronic media, a transaction for which the Secretary has adopted a standard under this part, the covered entity must conduct the transaction as a standard transaction.

(b) *Exception for direct data entry transactions.* A health care provider electing to use direct data entry offered by a health plan to conduct a transaction for which a standard has been adopted under this part must use the applicable data content and data condition requirements of the standard when conducting the transaction. The health care provider is not required to use the format requirements of the standard.

(c) *Use of a business associate.* A covered entity may use a business associate, including a health care clearinghouse, to conduct a transaction covered by this part. If a covered entity chooses to use a business associate to conduct all or part of a transaction on behalf of the covered entity, the covered entity must require the business associate to do the following:

(1) Comply with all applicable requirements of this part.

(2) Require any agent or subcontractor to comply with all applicable requirements of this part.

[65 FR 50367, Aug. 17, 2000, as amended at 74 FR 3325, Jan. 16, 2009]

§ 162.925 Additional requirements for health plans.

(a) *General rules.* (1) If an entity requests a health plan to conduct a transaction as a standard transaction, the health plan must do so.

(2) A health plan may not delay or reject a transaction, or attempt to adversely affect the other entity or the transaction, because the transaction is a standard transaction.

(3) A health plan may not reject a standard transaction on the basis that it contains data elements not needed or used by the health plan (for example, coordination of benefits information).

(4) A health plan may not offer an incentive for a health care provider to conduct a transaction covered by this part as a transaction described under the exception provided for in § 162.923(b).

(5) A health plan that operates as a health care clearinghouse, or requires an entity to use a health care clearinghouse to receive, process, or transmit a standard transaction may not charge fees or costs in excess of the fees or costs for normal telecommunications that the entity incurs when it directly transmits, or receives, a standard transaction to, or from, a health plan.

(6) During the period from March 17, 2009 through December 31, 2011, a health plan may not delay or reject a standard transaction, or attempt to adversely affect the other entity or the transaction, on the basis that it does not comply with another adopted standard for the same period.

(b) *Coordination of benefits.* If a health plan receives a standard transaction and coordinates benefits with another health plan (or another payer), it must store the coordination of benefits data it needs to forward the standard transaction to the other health plan (or other payer).

(c) *Code sets.* A health plan must meet each of the following requirements:

(1) Accept and promptly process any standard transaction that contains codes that are valid, as provided in subpart J of this part.

(2) Keep code sets for the current billing period and appeals periods still open to processing under the terms of the health plan's coverage.

[65 FR 50367, Aug. 17, 2000, as amended at 74 FR 3325, Jan. 16, 2009]

§ 162.930 Additional rules for health care clearinghouses.

When acting as a business associate for another covered entity, a health care clearinghouse may perform the following functions:

(a) Receive a standard transaction on behalf of the covered entity and translate it into a nonstandard transaction (for example, nonstandard format and/or nonstandard data content) for transmission to the covered entity.

(b) Receive a nonstandard transaction (for example, nonstandard format and/or nonstandard data content) from the covered entity and translate it into a standard transaction for transmission on behalf of the covered entity.

§ 162.940 Exceptions from standards to permit testing of proposed modifications.

(a) *Requests for an exception.* An organization may request an exception from the use of a standard from the Secretary to test a proposed modification to that standard. For each proposed modification, the organization must meet the following requirements:

(1) *Comparison to a current standard.* Provide a detailed explanation, no more than 10 pages in length, of how the proposed modification would be a significant improvement to the current standard in terms of the following principles:

(i) Improve the efficiency and effectiveness of the health care system by leading to cost reductions for, or improvements in benefits from, electronic health care transactions.

(ii) Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses.

(iii) Be uniform and consistent with the other standards adopted under this part and, as appropriate, with other private and public sector health data standards.

(iv) Have low additional development and implementation costs relative to the benefits of using the standard.

(v) Be supported by an ANSI-accredited SSO or other private or public organization that would maintain the standard over time.

(vi) Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster.

(vii) Be technologically independent of the computer platforms and transmission protocols used in electronic health transactions, unless they are explicitly part of the standard.

(viii) Be precise, unambiguous, and as simple as possible.

(ix) Result in minimum data collection and paperwork burdens on users.

(x) Incorporate flexibility to adapt more easily to changes in the health care infrastructure (such as new services, organizations, and provider types) and information technology.

(2) *Specifications for the proposed modification.* Provide specifications for the proposed modification, including any additional system requirements.

(3) *Testing of the proposed modification.* Provide an explanation, no more than 5 pages in length, of how the organization intends to test the standard, including the number and types of health plans and health care providers expected to be involved in the test, geographical areas, and beginning and ending dates of the test.

(4) *Trading partner concurrences.* Provide written concurrences from trading partners who would agree to participate in the test.

(b) *Basis for granting an exception.* The Secretary may grant an initial exception, for a period not to exceed 3 years, based on, but not limited to, the following criteria:

(1) An assessment of whether the proposed modification demonstrates a significant improvement to the current standard.

(2) The extent and length of time of the exception.

(3) Consultations with DSMOs.

(c) *Secretary's decision on exception.* The Secretary makes a decision and notifies the organization requesting the exception whether the request is granted or denied.

(1) *Exception granted.* If the Secretary grants an exception, the notification includes the following information:

(i) The length of time for which the exception applies.

(ii) The trading partners and geographical areas the Secretary approves for testing.

(iii) Any other conditions for approving the exception.

(2) *Exception denied.* If the Secretary does not grant an exception, the notification explains the reasons the Secretary considers the proposed modification would not be a significant improvement to the current standard and any other rationale for the denial.

(d) *Organization's report on test results.* Within 90 days after the test is completed, an organization that receives an

exception must submit a report on the results of the test, including a cost-benefit analysis, to a location specified by the Secretary by notice in the FEDERAL REGISTER.

(e) *Extension allowed.* If the report submitted in accordance with paragraph (d) of this section recommends a modification to the standard, the Secretary, on request, may grant an extension to the period granted for the exception.

Subpart J—Code Sets

§ 162.1000 General requirements.

When conducting a transaction covered by this part, a covered entity must meet the following requirements:

(a) *Medical data code sets.* Use the applicable medical data code sets described in § 162.1002 as specified in the implementation specification adopted under this part that are valid at the time the health care is furnished.

(b) *Nonmedical data code sets.* Use the nonmedical data code sets as described in the implementation specifications adopted under this part that are valid at the time the transaction is initiated.

§ 162.1002 Medical data code sets.

The Secretary adopts the following maintaining organization's code sets as the standard medical data code sets:

(a) For the period from October 16, 2002 through October 15, 2003:

(1) *International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2* (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following conditions:

(i) Diseases.

(ii) Injuries.

(iii) Impairments.

(iv) Other health problems and their manifestations.

(v) Causes of injury, disease, impairment, or other health problems.

(2) *International Classification of Diseases, 9th Edition, Clinical Modification, Volume 3 Procedures* (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:

(i) Prevention.

(ii) Diagnosis.

(iii) Treatment.

(iv) Management.

(3) *National Drug Codes* (NDC), as maintained and distributed by HHS, in collaboration with drug manufacturers, for the following:

(i) Drugs

(ii) Biologics.

(4) *Code on Dental Procedures and Nomenclature,* as maintained and distributed by the American Dental Association, for dental services.

(5) The combination of *Health Care Financing Administration Common Procedure Coding System (HCPCS),* as maintained and distributed by HHS, and *Current Procedural Terminology, Fourth Edition (CPT-4),* as maintained and distributed by the American Medical Association, for physician services and other health care services. These services include, but are not limited to, the following:

(i) Physician services.

(ii) Physical and occupational therapy services.

(iii) Radiologic procedures.

(iv) Clinical laboratory tests.

(v) Other medical diagnostic procedures.

(vi) Hearing and vision services.

(vii) Transportation services including ambulance.

(6) The *Health Care Financing Administration Common Procedure Coding System (HCPCS),* as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in health care services. These items include, but are not limited to, the following:

(i) Medical supplies.

(ii) Orthotic and prosthetic devices.

(iii) Durable medical equipment.

(b) For the period on and after October 16, 2003 through September 30, 2014:

(1) The code sets specified in paragraphs (a)(1), (a)(2),(a)(4), and (a)(5) of this section.

(2) *National Drug Codes (NDC),* as maintained and distributed by HHS, for reporting the following by retail pharmacies:

(i) Drugs.

(ii) Biologics.

(3) *The Healthcare Common Procedure Coding System (HCPCS),* as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in health care services, with the exception of drugs and biologics. These items include, but are not limited to, the following:

(i) Medical supplies.

(ii) Orthotic and prosthetic devices.

(iii) Durable medical equipment.

(c) For the period on and after October 1, 2014:

(1) The code sets specified in paragraphs (a)(4), (a)(5), (b)(2), and (b)(3) of this section.

(2) International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM) (including The Official ICD-10-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following conditions:

(i) Diseases.

(ii) Injuries.

(iii) Impairments.

(iv) Other health problems and their manifestations.

(v) Causes of injury, disease, impairment, or other health problems.

(3) International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS) (including The Official ICD-10-PCS Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:

(i) Prevention.

(ii) Diagnosis.

(iii) Treatment.

(iv) Management.

[65 FR 50367, Aug. 17, 2000, as amended at 68 FR 8397, Feb. 20, 2003; 74 FR 3362, Jan. 16, 2009; 77 FR 54720, Sept. 5, 2012]

§ 162.1011 Valid code sets.

Each code set is valid within the dates specified by the organization responsible for maintaining that code set.

Subpart K—Health Care Claims or Equivalent Encounter Information

§ 162.1101 Health care claims or equivalent encounter information transaction.

The health care claims or equivalent encounter information transaction is the transmission of either of the following:

(a) A request to obtain payment, and the necessary accompanying information from a health care provider to a health plan, for health care.

(b) If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care.

§ 162.1102 Standards for health care claims or equivalent encounter information transaction.

The Secretary adopts the following standards for the health care claims or equivalent encounter information transaction:

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drugs claims.* The National Council for Prescription Drug Programs (NCPDP) Telecommunication Standards Implementation Guide, Version 5, Release 1, September 1999, and equivalent NCPDP Batch Standards Batch Implementation Guide, Version

1, Release 1, (Version 1.1), January 2000, supporting Telecomunication Version 5.1 for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental, health care claims.* The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097. and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1. (Incorporated by reference in § 162.920).

(3) *Professional health care claims.* The ASC X12N 837—Health Care Claims: Professional, Volumes 1 and 2, Version 4010, may 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claims: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010x098A1. (Incorporated by reference in § 162.920).

(4) *Institutional health care claims.* The ASC X12N 837—Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096 and Addenda to Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X096A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1)(i) The standards identified in paragraph (a) of this section; and

(ii) For retail pharmacy supplies and professional services claims, the following: The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096, October 2002 (Incorporated by reference in § 162.920); and

(2)(i) *Retail pharmacy drug claims.* The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007 and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) *Dental health care claims.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006, ASC X12N/005010X224, and Type 1 Errata to Health Care Claim: Dental (837) ASC X12 Standards for Electronic Date Interchange Technical Report Type 3, October 2007, ASC X12N/005010X224A1. (Incorporated by reference in § 162.920.)

(iii) *Professional health care claims.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222. (Incorporated by reference in § 162.920.)

(iv) *Institutional health care claims.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12N/005010X223, and Type 1 Errata to Health Care Claim: Institutional (837) ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1. (Incorporated by reference in § 162.920.)

(v) *Retail pharmacy supplies and professional services claims.* (A) The Telecommunication Standard, Implementation Guide Version 5, Release 1, September 1999. (Incorporated by reference in § 162.920.)

(B) The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs (Incorporated by reference in § 162.920); and

(C) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222. (Incorporated by reference in § 162.920.)

(c) For the period on and after the January 1, 2012, the standards identified in paragraph (b)(2) of this section, except the standard identified in paragraph (b)(2)(v)(A) of this section.

[68 FR 8397, Feb. 20, 2003; 68 FR 11445, Mar. 10, 2003, as amended at 74 FR 3325, Jan. 16, 2009]

Subpart L—Eligibility for a Health Plan

§ 162.1201 Eligibility for a health plan transaction.

The eligibility for a health plan transaction is the transmission of either of the following:

(a) An inquiry from a health care provider to a health plan, or from one health plan to another health plan, to obtain any of the following information about a benefit plan for an enrollee:

(1) Eligibility to receive health care under the health plan.

(2) Coverage of health care under the health plan.

(3) Benefits associated with the benefit plan.

(b) A response from a health plan to a health care provider's (or another health plan's) inquiry described in paragraph (a) of this section.

§ 162.1202 Standards for eligibility for a health plan transaction.

The Secretary adopts the following standards for the eligibility for a health plan transaction:

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drugs.* The National Council for Prescription Drug Programs Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1), September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000 supporting Telecommunications Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental, professional, and institutional health care eligibility benefit inquiry and response.* The ASC X12N 270/271—Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092 and Addenda to Health Care Eligibility Benefit Inquiry and Response, Version 4010, October 2002, Washington Publishing Company, 004010X092A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011 both:

(1) The standards identified in paragraph (a) of this section; and

(2)(i) *Retail pharmacy drugs.* The Telecommunication Standard Implementation Guide Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) *Dental, professional, and institutional health care eligibility benefit inquiry and response.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Eligibility Benefit Inquiry and Response (270/271), April 2008, ASC X12N/005010X279. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8398, Feb. 20, 2003; 68 FR 11445, Mar. 10, 2003, as amended at 74 FR 3326, Jan. 16, 2009]

§ 162.1203 Operating rules for eligibility for a health plan transaction.

On and after January 1, 2013, the Secretary adopts the following:

(a) Except as specified in paragraph (b) of this section, the following CAQH CORE Phase I and Phase II operating rules (updated for Version 5010) for the eligibility for a health plan transaction:

(1) Phase I CORE 152: Eligibility and Benefit Real Time Companion Guide Rule, version 1.1.0, March 2011, and CORE v5010 Master Companion Guide Template. (Incorporated by reference in § 162.920).

(2) Phase I CORE 153: Eligibility and Benefits Connectivity Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(3) Phase I CORE 154: Eligibility and Benefits 270/271 Data Content Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(4) Phase I CORE 155: Eligibility and Benefits Batch Response Time Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(5) Phase I CORE 156: Eligibility and Benefits Real Time Response Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(6) Phase I CORE 157: Eligibility and Benefits System Availability Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(7) Phase II CORE 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule, version 2.1.0, March 2011. (Incorporated by reference in § 162.920).

(8) Phase II CORE 259: Eligibility and Benefits 270/271 AAA Error Code Reporting Rule, version 2.1.0. (Incorporated by reference in § 162.920).

(9) Phase II CORE 260: Eligibility & Benefits Data Content (270/271) Rule, version 2.1.0, March 2011. (Incorporated by reference in § 162.920).

(10) Phase II CORE 270: Connectivity Rule, version 2.2.0, March 2011. (Incorporated by reference in § 162.920).

(b) Excluding where the CAQH CORE rules reference and pertain to acknowledgements and CORE certification.

[76 FR 40496, July 8, 2011]

Subpart M—Referral Certification and Authorization

§ 162.1301 Referral certification and authorization transaction.

The referral certification and authorization transaction is any of the following transmissions:

(a) A request from a health care provider to a health plan for the review of health care to obtain an authorization for the health care.

(b) A request from a health care provider to a health plan to obtain authorization for referring an individual to another health care provider.

(c) A response from a health plan to a health care provider to a request described in paragraph (a) or paragraph (b) of this section.

[74 FR 3326, Jan. 16, 2009]

§ 162.1302 Standards for referral certification and authorization transaction.

The Secretary adopts the following standards for the referral certification and authorization transaction:

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drug referral certification and authorization.* The NCPDP Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1), September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000, supporting Telecommunications Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental, professional, and institutional referral certification and authorization.* The ASC X12N 278—Health Care Services Review—Request for Review and Response, Version 4010, May 2000, Washington Publishing Company, 004010X094 and Addenda to Health Care Services Review—Request for Review and Response, Version 4010, October 2002, Washington Publishing Company, 004010X094A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011 both—

(1) The standards identified in paragraph (a) of this section; and

(2)(i) *Retail pharmacy drugs.* The Telecommunication Standard Implementation Guide Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) *Dental, professional, and institutional request for review and response.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Services Review—Request for Review

and Response (278), May 2006, ASC X12N/005010X217, and Errata to Health Care Services Review-—Request for Review and Response (278), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X217E1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8398, Feb. 20, 2003, as amended at 74 FR 3326, Jan. 16, 2009]

Subpart N—Health Care Claim Status

§ 162.1401 Health care claim status transaction.

The health care claim status transaction is the transmission of either of the following:

(a) An inquiry from a health care provider to a health plan to determine the status of a health care claim.

(b) A response from a health plan to a health care provider about the status of a health care claim.

[74 FR 3326, Jan. 16, 2009]

§ 162.1402 Standards for health care claim status transaction.

The Secretary adopts the following standards for the health care claim status transaction:

(a) For the period from October 16, 2003 through March 16, 2009: The ASC X12N-276/277 Health Care Claim Status Request and Response, Version 4010, May 2000, Washington Publishing Company, 004010X093 and Addenda to Health Care Claim Status Request and Response, Version 4010, October 2002, Washington Publishing Company, 004010X093A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section; and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Status Request and Response (276/277), August 2006, ASC X12N/005010X212, and Errata to Health Care Claim Status Request and Response (276/277), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X212E1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3326, Jan. 16, 2009]

§ 162.1403 Operating rules for health care claim status transaction.

On and after January 1, 2013, the Secretary adopts the following:

(a) Except as specified in paragraph (b) of this section, the following CAQH CORE Phase II operating rules (updated for Version 5010) for the health care claim status transaction:

(1) Phase II CORE 250: Claim Status Rule, version 2.1.0, March 2011, and CORE v5010 Master Companion Guide, 00510, 1.2, March 2011. (Incorporated by reference in § 162.920).

(2) Phase II CORE 270: Connectivity Rule, version 2.2.0, March 2011. (Incorporated by reference in § 162.920).

(b) Excluding where the CAQH CORE rules reference and pertain to acknowledgements and CORE certification.

[76 FR 40496, July 8, 2011]

Subpart O—Enrollment and Disenrollment in a Health Plan

§ 162.1501 Enrollment and disenrollment in a health plan transaction.

The enrollment and disenrollment in a health plan transaction is the transmission of subscriber enrollment information from the sponsor of the insurance coverage, benefits, or policy, to a health plan to establish or terminate insurance coverage.

[74 FR 3327, Jan. 16, 2009]

§ 162.1502 Standards for enrollment and disenrollment in a health plan transaction.

The Secretary adopts the following standards for

enrollment and disenrollment in a health plan transaction.

(a) For the period from October 16, 2003 through March 16, 2009: ASC X12N 834—Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095 and Addenda to Benefit Enrollment and Maintenance, Version 4010, October 2002, Washington Publishing Company, 004010X095A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section; and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Benefit Enrollment and Maintenance (834), August 2006, ASC X12N/005010X220 (Incorporated by reference in § 162.920)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3327, Jan. 16, 2009]

Subpart P—Health Care Electronic Funds Transfers (EFT) and Remittance Advice

§ 162.1601 Health care electronic funds transfers (EFT) and remittance advice transaction.

The health care electronic funds transfers (EFT) and remittance advice transaction is the transmission of either of the following for health care:

(a) The transmission of any of the following from a health plan to a health care provider:

(1) Payment.

(2) Information about the transfer of funds.

(3) Payment processing information.

(b) The transmission of either of the following from a health plan to a health care provider:

(1) Explanation of benefits.

(2) Remittance advice.

[65 FR 50367, Aug. 17, 2000, as amended at 77 FR 1590, Jan. 10, 2012; 77 FR 48043, Aug. 10, 2012]

§ 162.1602 Standards for health care electronic funds transfers (EFT) and remittance advice transaction.

The Secretary adopts the following standards:

(a) For the period from October 16, 2003 through March 16, 2009: Health care claims and remittance advice. The ASC X12N 835—Health Care Claim Payment/Advice, Version 4010, May 2000, Washington Publishing Company, 004010X091, and Addenda to Health Care Claim Payment/Advice, Version 4010, October 2002, Washington Publishing Company, 004010X091A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both of the following standards:

(1) The standard identified in paragraph (a) of this section.

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221. (Incorporated by reference in § 162.920.)

(c) For the period from January 1, 2012 through December 31, 2013, the standard identified in paragraph (b)(2) of this section.

(d) For the period on and after January 1, 2014, the following standards:

(1) Except when transmissions as described in § 162.1601(a) and (b) are contained within the same transmission, for Stage 1 Payment Initiation transmissions described in § 162.1601(a), all of the following standards:

(i) The National Automated Clearing House Association (NACHA) Corporate Credit or Deposit Entry with Addenda Record (CCD+) implementation specifications as contained in the 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network as follows (incorporated by reference in § 162.920)—

(A) NACHA Operating Rules, Appendix One: ACH File Exchange Specifications; and

(B) NACHA Operating Rules, Appendix Three: ACH Record Format Specifications, Subpart 3.1.8 Sequence of Records for CCD Entries.

(ii) For the CCD Addenda Record (“7”), field 3, of the

standard identified in 1602(d)(1)(i), the Accredited Standards Committee (ASC) X12 Standards for Electronic Data Interchange Technical Report Type 3, "Health Care Claim Payment/Advice (835), April 2006: Section 2.4: 835 Segment Detail: "TRN Reassociation Trace Number," Washington Publishing Company, 005010X221 (Incorporated by reference in § 162.920).

(2) For transmissions described in § 162.1601(b), including when transmissions as described in § 162.1601(a) and (b) are contained within the same transmission, the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, "Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221. (Incorporated by reference in § 162.920).

[77 FR 1590, Jan. 10, 2012]

§ 162.1603 Operating rules for health care electronic funds transfers (EFT) and remittance advice transaction.

On and after January 1, 2014, the Secretary adopts the following for the health care electronic funds transfers (EFT) and remittance advice transaction:

(a) The Phase III CORE EFT & ERA Operating Rule Set, Approved June 2012 (Incorporated by reference in § 162.920) which includes the following rules:

(1) Phase III CORE 380 EFT Enrollment Data Rule, version 3.0.0, June 2012.

(2) Phase III CORE 382 ERA Enrollment Data Rule, version 3.0.0, June 2012.

(3) Phase III 360 CORE Uniform Use of CARCs and RARCs (835) Rule, version 3.0.0, June 2012.

(4) CORE-required Code Combinations for CORE-defined Business Scenarios for the Phase III CORE 360 Uniform Use of Claim Adjustment Reason Codes and Remittance Advice Remark Codes (835) Rule, version 3.0.0, June 2012.

(5) Phase III CORE 370 EFT & ERA Reassociation (CCD+/835) Rule, version 3.0.0, June 2012.

(6) Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012, except Requirement 4.2 titled "Health Care Claim Payment/Advice Batch Acknowledgement Requirements".

(b) ACME Health Plan, CORE v5010 Master Companion Guide Template, 005010, 1.2, March 2011 (incorporated by reference in § 162.920), as required by the Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012.

[77 FR 48043, Aug. 10, 2012]

Subpart Q—Health Plan Premium Payments

§ 162.1701 Health plan premium payments transaction.

The health plan premium payment transaction is the transmission of any of the following from the entity that is arranging for the provision of health care or is providing health care coverage payments for an individual to a health plan:

(a) Payment.

(b) Information about the transfer of funds.

(c) Detailed remittance information about individuals for whom premiums are being paid.

(d) Payment processing information to transmit health care premium payments including any of the following:

(1) Payroll deductions.

(2) Other group premium payments.

(3) Associated group premium payment information.

§ 162.1702 Standards for health plan premium payments transaction.

The Secretary adopts the following standards for the health plan premium payments transaction:

(a) For the period from October 16, 2003 through March 16, 2009: The ASC X12N 820—Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061, and Addenda to Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, October 2002, Washington Publishing Company, 004010X061A1.

(Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section, and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Payroll Deducted and Other Group Premium Payment for Insurance Products (820), February 2007, ASC X12N/005010X218. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3327, Jan. 16, 2009]

Subpart R—Coordination of Benefits

§ 162.1801 Coordination of benefits transaction.

The coordination of benefits transaction is the transmission from any entity to a health plan for the purpose of determining the relative payment responsibilities of the health plan, of either of the following for health care:

(a) Claims.

(b) Payment information.

§ 162.1802 Standards for coordination of benefits information transaction.

The Secretary adopts the following standards for the coordination of benefits information transaction.

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drug claims.* The National Council for Prescription Drug Programs Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1), September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000, supporting Telecommunications Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental health care claims.* The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097 and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1. (Incorporated by reference in § 162.920).

(3) *Professional health care claims.* The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claim: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X098A1. (Incorporated by reference in § 162.920).

(4) *Institutional health care claims.* The ASC X12N 837—Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096 and Addenda to Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X096A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standards identified in paragraph (a) of this section; and

(2)(i) *Retail pharmacy drug claims.* The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006, ASC X12N/005010X224, and Type 1 Errata to Health Care Claim: Dental (837), ASC X12 Standards for Electronic Date Interchange Technical Report Type 3, October 2007, ASC X12N/005010X224A1. (Incorporated by reference in § 162.920.)

(iii) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222.

(Incorporated by reference in § 162.920.)

(iv) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12N/005010X223, and Type 1 Errata to Health Care Claim: Institutional (837), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8399, Feb. 20, 2003, as amended at 74 FR 3327, Jan. 16, 2009]

Subpart S—Medicaid Pharmacy Subrogation

SOURCE: 74 FR 3328, Jan. 16, 2009, unless otherwise noted.

§ 162.1901 Medicaid pharmacy subrogation transaction.

The Medicaid pharmacy subrogation transaction is the transmission of a claim from a Medicaid agency to a payer for the purpose of seeking reimbursement from the responsible health plan for a pharmacy claim the State has paid on behalf of a Medicaid recipient.

§ 162.1902 Standard for Medicaid pharmacy subrogation transaction.

The Secretary adopts the Batch Standard Medicaid Subrogation Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007, National Council for Prescription Drug Programs, as referenced in § 162.1902 (Incorporated by reference at § 162.920):

(a) For the period on and after January 1, 2012, for covered entities that are not small health plans;

(b) For the period on and after January 1, 2013 for small health plans.

PART 164—SECURITY AND PRIVACY

Contents

Subpart A—General Provisions

§ 164.102 Statutory basis.
§ 164.103 Definitions.
§ 164.104 Applicability.
§ 164.105 Organizational requirements.
§ 164.106 Relationship to other parts.

Subpart B [Reserved]

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

§ 164.302 Applicability.
§ 164.304 Definitions.
§ 164.306 Security standards: General rules.
§ 164.308 Administrative safeguards.
§ 164.310 Physical safeguards.
§ 164.312 Technical safeguards.
§ 164.314 Organizational requirements.
§ 164.316 Policies and procedures and documentation requirements.
§ 164.318 Compliance dates for the initial implementation of the security standards.
Appendix A to Subpart C of Part 164—Security Standards: Matrix

Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information

§ 164.400 Applicability.
§ 164.402 Definitions.
§ 164.404 Notification to individuals.
§ 164.406 Notification to the media.
§ 164.408 Notification to the Secretary.
§ 164.410 Notification by a business associate.
§ 164.412 Law enforcement delay.
§ 164.414 Administrative requirements and burden of proof.

Subpart E—Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.
§ 164.501 Definitions.
§ 164.502 Uses and disclosures of protected health information: general rules.
§ 164.504 Uses and disclosures: Organizational requirements.
§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.
§ 164.508 Uses and disclosures for which an authorization is required.
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.
§ 164.514 Other requirements relating to uses and disclosures of protected health information.
§ 164.520 Notice of privacy practices for protected health information.
§ 164.522 Rights to request privacy protection for protected health information.
§ 164.524 Access of individuals to protected health information.
§ 164.526 Amendment of protected health information.
§ 164.528 Accounting of disclosures of protected health information.
§ 164.530 Administrative requirements.
§ 164.532 Transition provisions.
§ 164.534 Compliance dates for initial implementation of the privacy standards.

AUTHORITY: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)); and secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279.

SOURCE: 65 FR 82802, Dec. 28, 2000, unless otherwise noted.

Subpart A—General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104-191, and sections 13400-13424 of Public Law 111-5.

[78 FR 5692, Jan. 25, 2013]

§ 164.103 Definitions.

As used in this part, the following terms have the following meanings:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(D).

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(D).

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

[68 FR 8374, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009]

§ 164.104 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

§ 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) *Implementation specifications:*

(i) *Application of other provisions.* In applying a provision of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

(A) A reference in such provision to a "covered entity" refers to a health care component of the covered entity;

(B) A reference in such provision to a "health plan," "covered health care provider," or "health care clearinghouse," refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to "protected health information" refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to "electronic protected health information" refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

(B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with § 164.314 and § 164.504 regarding business associate arrangements and other organizational requirements.

(D) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates one or more health care components, it must include any component that would meet the definition of a covered entity or business associate if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions.

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.

(2) *Implementation specifications.*

(i) *Requirements for designation of an affiliated covered entity.*

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

(c)(1) *Standard: Documentation.* A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) *Implementation specification: Retention period .* A covered entity must retain the documentation as required by paragraph (c)(1) of this section

for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

[78 FR 5693, Jan. 25, 2013]

Subpart B [Reserved]

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

AUTHORITY: 42 U.S.C. 1320d-2 and 1320d-4; sec. 13401, Pub. L. 111-5, 123 Stat. 260.

SOURCE: 68 FR 8376, Feb. 20, 2003, unless otherwise noted.

§ 164.302 Applicability.

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

[78 FR 5693, Jan. 25, 2013]

§ 164.304 Definitions.

As used in this subpart, the following terms have the following meanings:

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subparts D or E of this part.)

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential authentication information composed of a string of characters.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

[68 FR 8376, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5693, Jan. 25, 2013]

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) *Flexibility of approach.*
(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) *Standards.* A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.

(d) *Implementation specifications.* In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

(*1*) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(*2*) Implement an equivalent alternative measure if reasonable and appropriate.

(e) *Maintenance.* A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of

electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).

[68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003; 78 FR 5693, Jan. 25, 2013]

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) *Information system activity review (Required).* Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3)(i) *Standard: Workforce security.* Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) *Implementation specifications:*

(A) *Authorization and/or supervision (Addressable).* Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) *Workforce clearance procedure (Addressable).* Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) *Termination procedures (Addressable).* Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4)(i) *Standard: Information access management.* Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) *Implementation specifications:*

(A) *Isolating health care clearinghouse functions (Required).* If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization (Addressable).* Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) *Access establishment and modification (Addressable).* Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right

of access to a workstation, transaction, program, or process.

(5)(i) *Standard: Security awareness and training.* Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications.* Implement:

(A) *Security reminders (Addressable).* Periodic security updates.

(B) *Protection from malicious software (Addressable).* Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring (Addressable).* Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management (Addressable).* Procedures for creating, changing, and safeguarding passwords.

(6)(i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents.

(ii) *Implementation specification: Response and reporting (Required).* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

(7)(i) *Standard: Contingency plan.* Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) *Implementation specifications:*

(A) *Data backup plan (Required).* Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan (Required).* Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan (Required).* Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) *Testing and revision procedures (Addressable).* Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis (Addressable).* Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

(3) *Implementation specifications: Written contract or other arrangement (Required).* Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that

meets the applicable requirements of § 164.314(a).

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.310 Physical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) *Standard: Facility access controls.* Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) *Implementation specifications:*

(i) *Contingency operations (Addressable).* Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) *Facility security plan (Addressable).* Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access control and validation procedures (Addressable).* Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) *Maintenance records (Addressable).* Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) *Standard: Workstation use.* Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) *Standard: Workstation security.* Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) *Standard: Device and media controls.* Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) *Implementation specifications:*

(i) *Disposal (Required).* Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) *Media re-use (Required).* Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) *Accountability (Addressable).* Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) *Data backup and storage (Addressable).* Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.312 Technical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) *Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) *Implementation specifications:*

(i) *Unique user identification (Required).* Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure (Required).* Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff (Addressable).* Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls.* Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) *Standard: Integrity.* Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) *Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).* Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(i) *Integrity controls (Addressable).* Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.314 Organizational requirements.

(a)(1) *Standard: Business associate contracts or other arrangements.* The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications (Required).*

(i) *Business associate contracts.* The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

(ii) *Other arrangements.* The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

(iii) *Business associate contracts with subcontractors.* The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b)(1) *Standard: Requirements for group health plans.* Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected

health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) *Implementation specifications (Required).* The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.316 Policies and procedures and documentation requirements.

A covered entity or business associate must, in accordance with § 164.306:

(a) *Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) *Standard: Documentation.* (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) *Implementation specifications:*

(i) *Time limit (Required).* Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability (Required).* Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) *Updates (Required).* Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.318 Compliance dates for the initial implementation of the security standards.

(a) *Health plan.* (1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) *Health care clearinghouse.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

Appendix A to Subpart C of Part 164—Security Standards: Matrix

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure (A)
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards(see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information

SOURCE: 74 FR 42767, Aug. 24, 2009, unless otherwise noted.

§ 164.400 Applicability.

The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.

§ 164.402 Definitions.

As used in this subpart, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

[78 FR 5695, Jan. 25, 2013]

§ 164.404 Notification to individuals.

(a) *Standard* —(1) *General rule.* A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) *Implementation specification: Timeliness of notification.* Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification* —(1) *Elements.* The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the

breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(2) *Plain language requirement.* The notification required by paragraph (a) of this section shall be written in plain language.

(d) *Implementation specifications: Methods of individual notification.* The notification required by paragraph (a) of this section shall be provided in the following form:

(1) *Written notice.* (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) *Substitute notice.* In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(B) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

(3) *Additional notice in urgent situations.* In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

§ 164.406 Notification to the media.

(a) *Standard.* For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

(b) *Implementation specification: Timeliness of notification.* Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.408 Notification to the Secretary.

(a) *Standard.* A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

(b) *Implementation specifications: Breaches involving 500 or more individuals.* For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site.

(c) *Implementation specifications: Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.410 Notification by a business associate.

(a) *Standard —*(1) *General rule.* A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

(b) *Implementation specifications: Timeliness of notification.* Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.412 Law enforcement delay.

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

§ 164.414 Administrative requirements and burden of proof.

(a) *Administrative requirements.* A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.

(b) *Burden of proof.* In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.

Subpart E—Privacy of Individually Identifiable Health Information

AUTHORITY: 42 U.S.C. 1320d-2, 1320d-4, and 1320d-9; sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); and secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279.

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of

this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

(d) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5695, Jan. 25, 2013]

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Health care operations means any of the following activities of the covered entity to the extent that the

activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Marketing: (1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is

reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) *Financial remuneration* means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Payment means:

(1) The activities undertaken by:

(i) Except as prohibited under § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 74 FR 42769, Aug. 24, 2009; 78 FR 5695, Jan. 25, 2013]

§ 164.502 Uses and disclosures of protected health information: General rules.

(a) *Standard.* A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Covered entities: Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).

(2) *Covered entities: Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

(3) *Business associates: Permitted uses and disclosures.* A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(4) *Business associates: Required uses and disclosures.* A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

(5) *Prohibited uses and disclosures.*

(i) *Use and disclosure of genetic information for underwriting purposes:* Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan*, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

(A) Except as provided in paragraph (a)(5)(i)(B) of this section:

(*1*) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(*2*) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(*3*) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and

(*4*) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

(B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

(ii) *Sale of protected health information:*

(A) Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.

(B) For purposes of this paragraph, sale of protected health information means:

(*1*) Except as provided in paragraph (a)(5)(ii)(B)(*2*) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

(*2*) Sale of protected health information does not include a disclosure of protected health information:

(*i*) For public health purposes pursuant to § 164.512(b) or § 164.514(e);

(*ii*) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

(*iii*) For treatment and payment purposes pursuant to § 164.506(a);

(*iv*) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

(*v*) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

(*vi*) To an individual, when requested under § 164.524 or § 164.528;

(*vii*) Required by law as permitted under § 164.512(a); and

(*viii*) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

(b) *Standard: Minimum necessary*

(1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) *Minimum necessary does not apply.* This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

(iii) Uses or disclosures made pursuant to an authorization under § 164.508;

(iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(v) Uses or disclosures that are required by law, as described by § 164.512(a); and

(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) *Standard: Uses and disclosures of protected health information subject to an agreed upon restriction.* A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) *Standard: Uses and disclosures of de-identified protected health information.*

(1) *Uses and disclosures to create de-identified information.* A covered entity may use protected health information to create information that

is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, *i.e.*, de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) *Implementation specification: Documentation.* The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

(g)(1) *Standard: Personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) *Implementation specification: adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3)(i) *Implementation specification: unemancipated minors.* If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

(C) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

(C) Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

(4) *Implementation specification: Deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) *Implementation specification: Abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) *Standard: Confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) *Standard: Uses and disclosures consistent with notice.* A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) *Standard: Disclosures by whistleblowers and workforce member crime victims*

(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 78 FR 5696, Jan. 25, 2013]

§ 164.504 Uses and disclosures: Organizational requirements.

(a) *Definitions.* As used in this section:

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Summary health information means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b)-(d) [Reserved]

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) *Implementation specifications: Business associate contracts with subcontractors.* The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: Uses and disclosures.* A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and

(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) *Standard: Requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5697, Jan. 25, 2013]

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent for uses and disclosures permitted.*

(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.* (1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5698, Jan. 25, 2013]

§ 164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: Authorizations for uses and disclosures* —(1) *Authorization required: General rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: Psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) *Authorization required: Marketing.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

(4) *Authorization required: Sale of protected health information.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart.
(ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

(b) *Implementation specifications: General requirements*

(1) *Valid authorizations.*

(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an

authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

(4) *Prohibition on conditioning of authorizations.* A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) *Implementation specifications: Core elements and requirements*

(1) Core elements. A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including

for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

(3) *Plain language requirement.* The authorization must be written in plain language.

(4) *Copy to the individual.* If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5699, Jan. 25, 2013]

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) *Standard: Use and disclosure for facility directories*

(1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

(B) The individual's location in the covered health care provider's facility;

(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and

(D) The individual's religious affiliation; and

(ii) Use or disclose for directory purposes such information:

(A) To members of the clergy; or

(B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) *Emergency circumstances.* (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) *Standard: Uses and disclosures for involvement in the individual's care and notification purposes*

(1) *Permitted uses and disclosures.*

(i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.

(2) *Uses and disclosures with the individual present.* If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) *Uses and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) *Uses and disclosures when the individual is deceased.* If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5699, Jan. 25, 2013]

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure

permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) *Standard: Uses and disclosures required by law.*

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: Uses and disclosures for public health activities.* (1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

(*1*) To conduct an evaluation relating to medical surveillance of the workplace; or

(*2*) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(*1*) By giving a copy of the notice to the individual at the time the health care is provided; or

(*2*) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains and documents the agreement to the disclosure from either:

(1) A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

(2) The individual, if the individual is an adult or emancipated minor.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: Disclosures about victims of abuse, neglect or domestic violence*

(1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(d) *Standard: Uses and disclosures for health oversight activities*

(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) *Joint activities or investigations.* Nothwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) *Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

(e) *Standard: Disclosures for judicial and administrative proceedings*

(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(*1*) No objections were filed; or

(*2*) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information , if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a *qualified protective order* means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Nothwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) *Other uses and disclosures under this section.* The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

(f) *Standard: Disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) *Permitted disclosures: Pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

(*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(*3*) De-identified information could not reasonably be used.

(2) *Permitted disclosures: Limited information for identification and location purposes.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) *Permitted disclosure: Victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) *Permitted disclosure: Decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) *Permitted disclosure: Crime on premises.* A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith

constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

(6) *Permitted disclosure: Reporting crime in emergencies.*

(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) *Standard: Uses and disclosures about decedents.*

(1) *Coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) *Funeral directors.* A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) *Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) *Standard: Uses and disclosures for research purposes*

(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(*1*) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(*2*) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(*3*) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) *Research on decedent's information.* The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) *Identification and date of action.* A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(*1*) An adequate plan to protect the identifiers from improper use and disclosure;

(*2*) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(*3*) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) *Standard: Uses and disclosures to avert a serious threat to health or safety*

(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) *Standard: Uses and disclosures for specialized government functions.*

(1) *Military and veterans activities*

(i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the FEDERAL REGISTER pursuant to paragraph (k)(1)(i) of this section.

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (*e.g.*, Executive Order 12333).

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual

was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12968;

(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) *Correctional institutions and other law enforcement custodial situations.*

(i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; or

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) *Covered entities that are government programs providing public benefits.*

(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(l) *Standard: Disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5700, Jan. 25, 2013]

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(a) *Standard: De-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) *Implementation specifications: Requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with

other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(*1*) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(*2*) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) *Implementation specifications: Re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) *Standard: Minimum necessary requirements.* In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

(2) *Implementation specifications: Minimum necessary uses of protected health information.*

(i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) *Implementation specification: Minimum necessary disclosures of protected health information.*

(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must

implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) *Implementation specifications: Minimum necessary requests for protected health information.*

(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(5) *Implementation specification: Other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) *Implementation specification: Limited data set:* A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Medical record numbers;

(viii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Device identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers;

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

(3) *Implementation specification: Permitted purposes for uses and disclosures.*

(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

(4) *Implementation specifications: Data use agreement*

(i) *Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(*1*) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(*2*) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(*3*) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(*4*) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(*5*) Not identify the information or contact the individuals.

(iii) *Compliance.*

(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1) Discontinued disclosure of protected health information to the recipient; and

(2) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

(f) *Fundraising communications.*

(1) *Standard: Uses and disclosures for fundraising.* Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

(ii) Dates of health care provided to an individual;

(iii) Department of service information;

(iv) Treating physician;

(v) Outcome information; and

(vi) Health insurance status.

(2) *Implementation specifications: Fundraising requirements.* (i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.

(ii) With each fundraising communication made to an individual under this paragraph, a covered entity must provide the

individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

(iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

(iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section.

(v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information.

(h)(1) *Standard: Verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) *Implementation specifications: Verification.*

(i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are

met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5700, Jan. 25, 2013]

§ 164.520 Notice of privacy practices for protected health information.

(a) *Standard: notice of privacy practices,*

(1) *Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) *Exception for group health plans.*

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) *Implementation specifications: Content of notice.*

(1) *Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

(ii) *Uses and disclosures.* The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications;

(B) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan; or

(C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan*, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.

(iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)(vi);

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) *Covered entity's duties.* The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) *Complaints.* The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) *Contact.* The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) *Optional elements.*

(i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii),

the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) *Implementation specifications: Provision of notice.* A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) *Specific requirements for health plans.*

(i) A health plan must provide the notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(v) If there is a material change to the notice:

(A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.

(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.

(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) *Specific requirements for electronic notice.*

(i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided

to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) *Implementation specifications: Joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013]

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) *Standard: Right of an individual to request restriction of uses and disclosures.*

(i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

(vi) A covered entity must agree to the request of an individual to restrict

disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate a restriction, if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.

(b)(1) *Standard: Confidential communications requirements.*

(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) *Implementation specifications: Conditions on providing confidential communications.*

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013]

§ 164.524 Access of individuals to protected health information.

(a) *Standard: Access to protected health information.*

(1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial*. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access*. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) *Implementation specifications: Requests for access and timely action*.

(1) *Individual's request for access*. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) *Timely action by the covered entity*. (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) *Implementation specifications: Provision of access*. If the covered entity provides an individual with

access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Providing the access requested*. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) *Form of access requested.*

(i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

(iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) *Time and manner of access.* (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

(4) *Fees*. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

(iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iv) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section.

(d) *Implementation specifications: Denial of access*. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Making other information accessible*. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) *Denial*. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) *Other responsibility*. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) *Implementation specification: Documentation*. A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

[65 FR 82823, Dec. 28, 2000, as amended at 78 FR 5701, Jan. 25, 2013]

§ 164.526 Amendment of protected health information.

(a) *Standard: Right to amend*. (1) *Right to amend*. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment*. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: Requests for amendment and timely action*.

(1) *Individual's request for amendment*. The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity*.

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: Accepting the amendment*. If the covered entity accepts the requested amendment, in whole or in part, the

covered entity must comply with the following requirements.

(1) *Making the amendment*. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual*. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others*. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: Denying the amendment*. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial*. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) *Statement of disagreement*. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement*. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping*. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures*. (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: Actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: Documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.

(a) *Standard: Right to an accounting of disclosures of protected health information.* (1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in § 164.506;

(ii) To individuals of protected health information about them as provided in § 164.502;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;

(iv)Pursuant to an authorization as provided in § 164.508;

(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;

(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);

(viii) As part of a limited data set in accordance with § 164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) *Implementation specifications: Content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the

same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) *Implementation specifications: Provision of the accounting.* (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002]

§ 164.530 Administrative requirements.

(a)(1) *Standard: Personnel designations.* (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) *Implementation specification: Personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) *Standard: Training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) *Implementation specifications: Training.* (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) *Standard: Safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) *Implementation specification: Safeguards.* A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

(d)(1) *Standard: Complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

(2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) *Standard: Sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) *Implementation specification: Documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) *Standard: Mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) *Standard: Refraining from intimidating or retaliatory acts.* A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

(2) Must refrain from intimidation and retaliation as provided in § 160.316 of this subchapter.

(h) *Standard: Waiver of rights.* A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) *Standard: Policies and procedures.* A covered entity must implement policies and procedures

with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) *Standard: Changes to policies and procedures.* (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) *Implementation specification: Changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) *Implementation specifications: Changes to privacy practices stated in the notice.* (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) *Implementation specification: Changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) *Standard: Documentation.* A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(iv) Maintain documentation sufficient to meet its burden of proof under § 164.414(b).

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation

required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) *Standard: Group health plans.* (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 71 FR 8433, Feb. 16, 2006; 74 FR 42769, Aug. 24, 2009]

§ 164.532 Transition provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with § 164.512(i)(1)(i).

(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).

(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research;

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or

(4) A waiver of authorization in accordance with § 164.512(i)(1)(i).

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance.* (1) *Qualification.* Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or

(ii) September 22, 2014.

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

(f) *Effect of prior data use agreements.* If, prior to January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e), notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of:

(1) The date such agreement is renewed or modified on or after September 23, 2013; or

(2) September 22, 2014.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 78 FR 5702, Jan. 25, 2013]

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following as applicable:

(1) *Health plans other han small health plans.* April 14, 2003.

(2) *Small health plans.* April 14, 2004.

(c) *Health clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.

[66 FR 12434, Feb. 26, 2001]

INITIAL HIPAA COMPLIANCE CHECKLIST

You can use this Checklist to make sure you have completed all the necessary initial forms. When completed, place a checkmark on the blank line next to the form that has been completed. Not all of the forms in the notebook need to be completed immediately; however, the forms listed below should be completed as soon as possible in order to document your compliance with the HIPAA medical privacy rules:

☐ **(1)** **Notice of Privacy Practices.** All covered employees should receive the Notice of Privacy Practices for the Barton County Community College Medical, Dental, and Prescription Plan, Barton County Community College Level II Preventive Health Benefits Plan, and Barton Community College Health Flexible Spending Account immediately. After you have distributed this Notice initially to all covered employees, you should distribute the Reminder Notice annually at open enrollment (see (2) below). Keep in mind, the Notice of Privacy Practices need only go to covered employees (that is, covered spouses and dependents do not need to be provided a separate notice).

☐ **(2)** **Reminder of the Notice of Privacy Practices (behind Notices of Privacy Practices).** Once you have distributed the entire Notice of Privacy Practices, distribute the Reminder of the Notice of Privacy Practices annually at open enrollment to covered employees.

☐ **(3)** **Training Log (Exhibit 14 behind HIPAA Privacy Policy and Procedures).** As soon as an "authorized employee" is trained on the HIPAA medical privacy rules and the policies and procedures, the "authorized employee" should sign the Training Log. All "authorized employees" need to be trained before seeing PHI.

☐ **(4)** **Employee Acknowledgment (Exhibit 15 behind HIPAA Privacy Policy and Procedures).** As soon as an "authorized employee" is trained on the HIPAA medical privacy rules and the policies and procedures, the trained "authorized employee" should sign the individual Employee Acknowledgment form.

☐ **(5)** **HIPAA Security Compliance – Risk Analysis Worksheet (Exhibit 16 behind HIPAA Privacy Policy and Procedures).** The Risk Analysis Worksheet should be completed as soon as possible in order to comply with HIPAA's electronic security rules.

☐ **(6)** **Organized Health Care Arrangement Designation Form (Tab 1 behind Miscellaneous Administrative Forms).** In order to simply your HIPAA medical privacy compliance, all group health plans which receive PHI are combined into an "organized health care arrangement" or "OHCA." This is why you only need one set of policies and procedures despite having more than one group health plan subject to the full extent of the privacy rules. This Form should be signed and dated.

☐ **(7)** **Hybrid Entity Designation Form (Tab 2 behind Miscellaneous Administrative Forms).** Your plan is an "umbrella" plan potentially made up of non-group health plans, group health plans from which you receive no PHI, and one or

more group health plans from which you receive PHI and for which you need policies and procedures. The Hybrid Entity Designation Form "carves out" the group health plan(s) to which the full extent of the privacy rules apply from all other "sub-plans" in the plan. This Form documenting how your compliance system is set up should be signed and dated.

☐ **(8)** **Designation and Acceptance Forms (Tabs 3, 4, and 5 behind Miscellaneous Administrative Forms).** There is a Designation and Acceptance Form for the Privacy Officer, Contact Person and Security Officer. The individual(s) "wearing those hats" should read through the Forms and the bullet points which outline their duties and responsibilities and then sign and date the Form(s).

☐ **(9)** **Technical and Physical Safeguard Worksheet (Tab 6 behind Miscellaneous Administrative Forms).** In order to help you consider where all PHI is located and to document how you have chosen to safeguard the PHI that you have, you need to complete the Technical and Physical Safeguard Worksheet.

☐ **(10)** **HIPAA Privacy & Security Safeguards – Checklist (Tab 7 behind Miscellaneous Administrative Forms).** In order to help you complete the Technical and Physical Safeguard Worksheet (see (9) above) and to help you brainstorm potential safeguards that could be used and documented on the Worksheet, you should analyze the Checklist of HIPAA Privacy & Security Safeguards – Checklist and put a checkmark next to the safeguards you implement.

☐ **(11)** **Business Associate Worksheet (Tab 8 behind Miscellaneous Administrative Forms).** Please document information regarding all of your business associates and the business associate agreements you have with them on the Worksheet.