THE PRIVACY OFFICER'S HANDBOOK

Second Edition

MARY D. BRANDT, MBA, RHIA, CHE, CHPS

HCPro

The Privacy Officer's Handbook, Second Edition, is published by HCPro, Inc.

ISBN: 978-1-60146-723-2

Mary D. Brandt, MBA, RHIA, CHE, CHPS, Author
Gerianne Spanek, Managing Editor
Ilene MacDonald, CPC, Executive Editor
Lauren McLeod, Group Publisher
Mike Mirabello, Senior Graphic Artist
Amanda Donaldson, Copyeditor
Karin Holmes, Proofreader
Matt Sharpe, Production Supervisor
Susan Darbyshire, Art Director
Jean St. Pierre, Director of Operations

Advice given is general. Readers should consult professional counsel for specific legal, ethical, or clinical questions. Arrangements can be made for quantity discounts. For more information, contact:

HCPro, Inc.
P.O. Box 1168
Marblehead, MA 01945
Telephone: 800/650-6787 or 781/639-1872
Fax: 781/639-2982
E-mail: *customerservice@hcpro.com*

Visit HCPro at its World Wide Web sites:
www.hcpro.com* and *www.hcmarketplace.com

12/2009
21742

Contents

About the Author

Mary D. Brandt, MBA, RHIA, CHE, CHPS

Mary D. Brandt, MBA, RHIA, CHE, CHPS, a nationally recognized expert on patient privacy, information security, and regulatory compliance, is associate executive director of health information management (HIM) at Scott & White Healthcare in Temple, TX. Some of her publications were used as a basis for the Health Insurance Portability and Accountability Act of 1996 privacy regulations.

Until recently, Brandt served as president of Brandt & Associates, a healthcare consulting firm in Bellaire, TX, that provided services to a wide range of clients. Previously, she provided consulting services for PricewaterhouseCoopers and a large healthcare IT company. As the former director of policy and research for the American Health Information Management Association (AHIMA), she worked with standards development organizations to address privacy and confidentiality issues and to develop standards for computer-based patient records.

Brandt has published more than 30 articles, 25 position statements/practice briefs, and three sets of practice guidelines on HIM issues, including information security and computer-based patient records. She is a regular contributor to **Health Information Compliance Insider,** a monthly print and electronic newsletter published by HCPro, Inc.

Brandt holds a BS in medical record administration, an MBA, and certifications by AHIMA and the American College of Healthcare Executives. She is a past recipient of AHIMA's Legacy Award for her contributions to the professional body of knowledge.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the federal law that forms the basis for administrative simplification in healthcare. This introduction provides an overview of HIPAA, the covered entities (CE) that must comply, and the three sets of regulations that implement it:

- Transactions and code sets
- Security
- Privacy

The American Recovery and Reinvestment Act of 2009 (ARRA) contains additional requirements relating to privacy and security. Title XIII, the Health Information Technology for Economic and Clinical Health Act (HITECH), provides funding for the adoption of healthcare information technology and addresses ongoing privacy issues.

Overview

HIPAA

HIPAA, or Public Law 104-191, was signed into law August 21, 1996. The original purpose of this federal law was to make it easier for people to take their health insurance coverage with them when they changed jobs, thus the reference to "health insurance portability." (The HIPAA Administrative Simplification Rules are codified in 45 *CFR* Parts 160, 162, and 164.)

The law includes several other provisions, including administrative simplification, which have had a major impact on the healthcare industry. The purpose of administrative simplification is to improve the efficiency and effectiveness of the healthcare system by requiring national standards for electronic healthcare transactions. At the same time, Congress recognized that increasing the use of electronic technology could erode the privacy of health information. So Congress added provisions to HIPAA to require federal privacy protections for individually identifiable health information.

For the first time, the Privacy Rule established a foundation of federal protections for the privacy of health information. Previously, protections for health information were provided by a patchwork of state laws, some of which offered good privacy protections, and others that offered few, if any, protections.

ARRA

Enacted February 17, 2009, ARRA (sometimes called the stimulus bill) includes HITECH, which focuses on promoting electronic communication in healthcare, such as electronic health records (EHR).

HITECH also amended the HIPAA Privacy and Security Rules. These changes include:

- Increased penalties—generally effective February 2009
- New breach notification rules—the interim final rule was published August 24, 2009, and became effective September 23, 2009
- New rules for restrictions requested by individuals—generally effective February 2010
- New prohibitions on the sale of protected health information (PHI)—generally effective February 2011
- Other rules pertaining to EHRs, including accounting of disclosures—generally effective January 2011 (can be later)

Note that ARRA is a statute, not a regulation. Some of its provisions must be followed directly, whereas others will require interpretation, regulation, or guidance, which ARRA describes. Like other statutes, ARRA requires additional regulations or written guidance to clarify its provisions and mandates.

Definitions

Several definitions, as stated in HIPAA and the Privacy Rule, are important for understanding HIPAA's requirements. Generally, ARRA follows the definitions outlined in HIPAA and the Privacy Rule. In a few cases, however, ARRA provides additional definitions, which are highlighted with the NEW icon. This icon highlights new information throughout the book.

Several definitions included in the law are important for understanding HIPAA's requirements (45 *CFR* §§160.103 and 162.103).

Code set: Any set of codes used for encoding data elements, such as medical diagnosis or procedure codes.

Healthcare clearinghouse: A public or private entity that processes nonstandard data elements of health information into standard data elements.

Healthcare provider: A provider of medical or health services or supplies.

Health information: Any information, whether oral or recorded, in any form or medium that:

- Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse
- Relates to the past, present, or future physical or mental health of an individual or the past, present, or future payment for the provision of care to an individual

Health plan: Individual or group plan that provides or pays the cost of medical care, including:

- Health maintenance organizations
- Medicare program
- State Medicaid programs
- Indian Health Service

Covered Entities

CEs are the organizations or individuals that must comply with HIPAA. They are:

- Health plans (with the exception of the workers' compensation program)
- Healthcare clearinghouses
- Healthcare providers that transmit health information in electronic form using standard transactions

Note that not all healthcare providers are CEs. Only those providers that transmit health information electronically as part of a standard transaction are CEs. Generally, this means that healthcare providers that bill electronically are CEs. Healthcare providers that do their billing on paper and use the telephone to obtain authorization for services are not CEs pursuant to HIPAA.

Transactions and Code Sets

The good old days

Before standard transactions were required under HIPAA, payers were free to create their own requirements. Providers that wanted to receive payment from an insurance company had to bill in a format dictated by the insurance company. Not surprisingly, this greatly increased the cost and complexity of healthcare administrative processes. It is estimated that there were more than 400 formats in use just for filing healthcare claims.

New rules

Now, HIPAA requires both payers and providers to use standard formats for electronic financial and administrative transactions and code sets.

Nine types of electronic transactions have standardized formats:

- Health claims or encounters
- Health claims attachments
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Healthcare payment and remittance advice
- Health plan premium payments
- First report of injury
- Health claim status
- Referral certification and authorization

Both payers and providers must use the designated standards for these transactions. Further, both parties must use the standard format when sending transactions; neither sender nor recipient may change it.

Note: Except for Medicare claims, providers are not required to use electronic transactions. If they transmit information electronically using covered transactions, they must follow the standard format for those transactions.

Healthcare providers that cannot send transactions in the standard format may use a healthcare clearinghouse to transform their nonstandard transactions into standard formats and submit them to payers. Similarly, payers that cannot accept transactions in the standard format may also use a healthcare clearinghouse to receive standard transactions on their behalf.

Unique identifiers

HIPAA also requires that unique identifiers be established for:

- Individuals (this is pending and is not likely to be resolved for some time)
- Employers (this is the federal Employer Identification Number)
- Health plans (this is the federal Health Plan ID)
- Healthcare providers (this is the federal Provider ID)

Electronic signature

HIPAA also requires the U.S. Department of Health and Human Services (HHS) to establish standards for electronic signatures. The proposed security regulations specified use of a digital signature using public key/private key encryption. This requirement, which is pending further study, is not included in the final security regulations.

Security Regulations

HIPAA required HHS to develop security standards for health information to:

- Ensure the integrity and confidentiality of the information, and
- Protect against any reasonably anticipated threats or hazards or unauthorized uses or disclosures.

Privacy Regulations

In addition to standards for transactions and security, HIPAA also required HHS to develop privacy standards for health information. These standards are designed to address:

- Individuals' rights with respect to their health information
- Procedures that should be established for exercise of these rights
- Uses and disclosures of information as authorized or required by law

Details of the Privacy Rule are described in Chapters 2–18. Additional requirements have been incorporated into chapters containing information affected by ARRA, specifically Chapters 1, 2, 3, 6, 7, 8, 11, and 17.

Where Privacy and Security Overlap

Although HIPAA's Privacy Rule and Security Rule address two different aspects of compliance, there are some overlapping or complementary standards between the two. ARRA provides additional requirements in some areas, as illustrated in Figure I.1 in the Appendix.

Penalties for Noncompliance

HIPAA

Generally, HHS may impose a penalty of $100 for each violation of a privacy, security, or transaction regulation. Total penalties for all violations of an identical requirement during a calendar year may be as much as $25,000.

For wrongful disclosure of individually identifiable health information, a person may face one or both of the following penalties:

- Fine of up to $50,000
- Imprisonment for up to one year

For wrongful disclosure of individually identifiable health information for commercial advantage, personal gain, or malicious harm, a person may face one or both of the following penalties:

- Fine of up to $250,000
- Imprisonment for up to 10 years

ARRA

New provisions in ARRA expand enforcement by making individuals, not just entities, subject to penalties. This change is meant to override a previous letter issued by the U.S. Department of Justice that suggested individuals could not be convicted under HIPAA. Pursuant to ARRA, there are new penalties for "noncompliance due to willful neglect," and penalties may be as high as $1.5 million annually.

Effect on State Law

Although HIPAA and its implementing regulations are federal law, they do not automatically supersede or preempt state law and regulation. State law or regulation will control if the provision is necessary for:

- Prevention of fraud and abuse
- Appropriate state regulation of insurance and health plans
- State reporting on healthcare delivery or costs
- Addressing controlled substances
- Public health reporting or investigation of diseases, injuries, births, deaths, or child abuse
- Health plan reporting for financial audits or program monitoring
- Facility or individual licensure or certification

And, like HIPAA, ARRA does not automatically preempt state law and regulation.

This presents a special challenge to privacy officers. Understanding and complying with federal laws and regulations isn't enough. You must also be knowledgeable with respect to state laws and regulations and understand which one prevails. Generally, you must comply with the more stringent requirement, regardless of whether it is state or federal.

Remember that HIPAA establishes a floor, not a ceiling, for privacy protections. You must continue to comply with state laws and regulations, especially when they provide greater privacy protections or greater rights to individuals with respect to their health information.

Resources

1. HIPAA and its implementing regulations are available on the Internet. Access them at the Office for Civil Rights (OCR) Health Information Privacy Web site *(www.hhs.gov/ocr/privacy)*. Click on HIPAA Administrative Simplification Statute and Rules on the left, then select from the following:
   - Privacy Rule
   - Transactions and Code Set Standards
   - Employer Identifier Standard
   - National Provider Identifier Standard
   - Security Rule
   - Enforcement Rule

   Note: The Privacy Rule has undergone many changes, with various versions of the rule published December 28, 2000; December 29, 2000; August 14, 2002; and February 16, 2005. For ease in reference, print the unofficial version of the Combined Regulation Text of All Rules at the address provided in the previous paragraph. For the official version, refer to 45 *CFR* Parts 160, 162, and 164, which was pending at the time of this publication.

2. For help determining whether an organization is a CE under HIPAA, visit the OCR Health Information Privacy Web site. From the box on the left side of the page, select Understanding HIPAA Privacy. Then select For Covered Entities and scroll down to Are You a Covered Entity?

3. The federal ARRA law and implementing regulations are also available on the Internet. For the full text of the law, visit the Library of Congress' Thomas Web site at *www.thomas.loc.gov* and search for Public Law 111-5.

4. Implementing regulations for privacy pursuant to ARRA will be published by HHS and posted on the OCR Health Information Privacy Web site.

CHAPTER

1

Overview of the HIPAA Privacy Rule and ARRA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule gives patients and their personal representatives significant rights with respect to their health information. The American Recovery and Reinvestment Act of 2009 (ARRA) contains additional privacy legislation necessary to support widespread implementation of healthcare information technology.

This chapter takes a high-level look at major privacy requirements, including definitions of key terms and patients' rights. The regulations are detailed and complex. The purpose of this chapter is to provide a general understanding of the many requirements with which you must comply. Chapters 2–18 discuss specific areas of compliance in greater detail.

Overview

The *Standards for Privacy of Individually Identifiable Health Information* (also known as the Privacy Rule) establishes a set of national standards for the protection of certain health information (45 *CFR* Parts 160 and 164). This is the first time such protections have existed at the federal level.

The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement HIPAA's privacy requirements. The Privacy Rule describes requirements for the use and disclosure of individuals' health information—protected health information (PHI)—by organizations subject to the Privacy Rule—covered entities (CE). The rule also gives individuals significant rights to understand and control how their health information is used.

HHS' Office for Civil Rights (OCR) is responsible for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

Definitions

Several definitions, as stated in HIPAA and the Privacy Rule, are important for understanding HIPAA's requirements. Generally, ARRA follows the definitions outlined in HIPAA and the Privacy Rule. In a few cases, however, ARRA provides additional definitions, which are highlighted with the NEW icon.

NEW ***Breach:*** Unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information, except when an unauthorized person to whom the information is disclosed would not reasonably have been able to retain the information.

The term "breach" does not include any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a CE or business associate (BA) if one of the following applies:

- The acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship with the CE or BA and the information is not further acquired, accessed, used, or disclosed by any person
- Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a CE or BA to another similarly situated individual at the same facility, and any such information received as the result of the disclosure is not further acquired, accessed, used, or disclosed without authorization by any person

Covered entities: The organizations or individuals that must comply with HIPAA. They are health plans (with the exception of workers' compensation programs), healthcare clearinghouses, and healthcare providers that transmit health information in electronic form using standard transactions.

NEW ***Electronic health record (EHR):*** An electronic record of health-related information about an individual that is created, gathered, managed, or consulted by authorized healthcare clinicians and staff members.

Designated record set: Information used by a CE to make decisions about individuals. For providers, the designated record set includes medical records and billing records. For health plans, the designated record set includes enrollment, payment, claims adjudication, and case or medical management records.

***Identifiers for PHI*:** PHI is considered "identifiable" if it contains any one of 18 specific identifiers of individuals and their relatives, employers, or household members, including:

- Names
- Geographic subdivisions smaller than a state
- All elements of dates (except year) for birth, admission, discharge, and death
- All ages over 89, including year
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Device identifiers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographs

***Healthcare operations*:** Healthcare business activities, including quality assessment, case management, care coordination, peer review, training of students, accreditation, certification, licensing and credentialing activities, policy underwriting or premium rating, legal services, auditing functions, and business planning and development.

***Payment*:** Activities involving payment for healthcare services.

NEW ***Personal health record (PHR)*:** An electronic record of identifiable health information about an individual that can be drawn from multiple sources and is managed, shared, or controlled by or primarily for the individual.

***Protected health information*:** This is information that:

- Identifies an individual
- Relates to the individual's health, healthcare treatment, or healthcare payment
- Is maintained or disclosed verbally, electronically, or on paper

***Treatment*:** Provision, coordination, or management of healthcare services for an individual by one or more healthcare providers.

NEW ***Vendor of personal health records:*** An entity, other than a CE, that offers or maintains a PHR.

General Rule for Uses and Disclosures

The Privacy Rule defines and limits the circumstances in which an individual's PHI may be used or disclosed by CEs.

A CE may use or disclose PHI only as:

- Permitted or required by the Privacy Rule; or
- Authorized in writing by individuals who are the subject of the PHI or their personal representatives.

Required disclosures

The Privacy Rule permits a number of disclosures, but it requires CEs to disclose PHI in only two situations. A CE must disclose PHI to:

- Individuals or their personal representatives when they request access to their PHI or an accounting of disclosures
- HHS for compliance investigations or review or enforcement actions

State law or regulation may require additional disclosures (such as the reporting of communicable diseases or suspected abuse and neglect), and CEs must comply with applicable state laws and regulations, in addition to the Privacy Rule.

Permitted disclosures

A CE is permitted—but not required—to use and disclose PHI without the individual's authorization in several situations, as described in the following section.

Uses and disclosures for treatment, payment, and healthcare operations

A CE may use or disclose PHI for its own treatment, payment, or healthcare operations.

A CE may also disclose PHI for the:

- Treatment activities of any healthcare provider;
- Payment activities of another CE or any healthcare provider; or
- Healthcare operations of another CE for quality assurance or competency reviews or fraud and abuse compliance activities. In this case, both CEs must have had a relationship with the individual and the PHI must pertain to the relationship.

The patient's authorization is not required for these uses or disclosures.

Other uses and disclosures

Authorization for use and disclosure

Generally, the patient's written authorization is necessary to disclose PHI, except:

- For treatment, payment, or healthcare operations
- When the disclosure is required or permitted by law
- For research, if the requirement for authorization is waived by an institutional review board

Agree or object

In some situations, patients' written authorization is unnecessary, but they must be told about the use or disclosure and given an opportunity to agree or object. These uses or disclosures include using patients' information in a facility directory and sharing information with the patients' family and friends.

Authorization not required; opportunity to agree or object not required

When a disclosure is required by law, the patient does not have to give written authorization for the disclosure or be given the opportunity to agree or object. For example, state law may require that healthcare

providers report cases of tuberculosis to the local public health department. Providers aren't required to give patients an opportunity to agree or object to this disclosure or obtain their written authorization before reporting this information.

Minimum necessary

When using or disclosing PHI, CEs must make reasonable efforts to limit the PHI to the least amount needed to accomplish the intended purpose. When requesting PHI from each other, CEs must also limit the amount of PHI requested to the minimum amount needed.

The minimum necessary requirement does not apply to:

- Provider requests for treatment information;
- Requests from the individual or his personal representative;
- Disclosures made based on authorization;
- Disclosures made to HHS for a complaint investigation, compliance review, or enforcement; or
- Disclosures required by law.

When providers request PHI for treatment purposes, you should provide whatever information they request.

Because CEs are required to request the minimum amount of information needed, you may rely on another CE's request as being the minimum necessary.

Patient Rights

The HIPAA Privacy Rule, for the first time at the federal level, gives patients significant rights with respect to their health information. For ease in reference, these rights are listed here alphabetically.

Access to PHI

Individuals have the right to inspect and obtain a copy of their PHI in a designated record set for as long as the CE maintains information. Generally, the Privacy Rule requires CEs to retain documentation for at least six years. Most healthcare organizations keep medical records for much longer time periods, and individuals have the right to access their records for as long as the CE keeps them.

CEs may ask that requests be in writing. Generally, organizations ask individuals to complete a standard authorization form authorizing release of the information directly to the individual.

Requests for access may be denied in a few, very limited circumstances, as described in Chapter 2.

CEs may not charge individuals a fee for retrieving their records or for simply reviewing their records. They may charge reasonable, cost-based fees for copying, mailing, and preparing a summary of the information, if individuals request it.

NEW ARRA also addresses copy fees to individuals. The law allows individuals to obtain an electronic copy of their records from providers with electronic record systems, and it allows providers to charge a fee for the labor associated with fulfilling the request. Additional regulations in this area were pending at the time of publication.

Accounting of disclosures

Pursuant to HIPAA, an individual has the right to receive an accounting for certain types of disclosures of PHI for up to six years prior to the request. (The request for an accounting cannot be earlier than the date the Privacy Rule became effective, which was April 14, 2003, for most CEs.)

Examples of disclosures that must be included in an accounting are:

- Submission of reports required by law, such as abuse/neglect, gunshot wounds, births, deaths and immunizations;
- Notifying coroners, medical examiners and organ donation agencies of deaths; and
- Responding to court orders, warrants, and subpoenas (unless the individual authorized the disclosure).

CEs are not required to account for many of the disclosures they make, including disclosures:

- For treatment, payment, or healthcare operations;
- To the individual or his or her personal representative;
- Authorized by the individual or his or her personal representative;
- For the facility's directory or to those involved in the individual's care;

- For national security or intelligence purposes; and
- To correctional institutions or law enforcement officials regarding inmates or individuals in lawful custody.

New requirements under ARRA make accounting of disclosures even more daunting. CEs that use EHR systems must account for all disclosures if the individual asks them to do so. This includes disclosures for treatment, payment, and healthcare operations, which are exempt under HIPAA. The HHS secretary will define a standard for the accounting and issue regulations for compliance. Those regulations were pending at the time of publication. The effective dates depend on when an entity purchased its EHR system, with the earliest date of compliance being January 1, 2011.

Refer to Chapter 3 for additional details.

Amendments to PHI

Individuals have the right to request a CE to amend PHI:

- In a designated record set
- For as long as the CE maintains information

The CE may require a written request with the rationale for making the change. (This is a good practice because requests for amendment are sometimes long, rambling, and difficult to comprehend.)

Although individuals have the right to request an amendment to their PHI, CEs are not required to grant the request. CEs may deny requests in certain situations, but they must adhere to specific procedures when doing so.

Refer to Chapter 4 for additional details.

Confidential communications

Individuals have the right to ask to receive communications of PHI by an alternative means or at an alternative location. CEs must accommodate reasonable requests.

For example:

- Individuals ask to be called on a cell phone instead of at home for appointment reminders and test results
- Individuals ask to have bills sent to their offices instead of their homes

Refer to Chapter 8 for additional information.

Notice of Privacy Practices

Individuals have a right to receive a notice of the CE's privacy practices. The notice must be written in plain language and describe the ways in which the CE may use or disclose PHI. The notice must also describe individuals' rights with respect to their health information, including the right to complain to HHS and to the CE if they believe their privacy rights have been violated.

In addition to providing the notice, covered healthcare providers must obtain written acknowledgment of receipt of the notice from patients. If acknowledgment cannot be obtained due to emergency circumstances, inability to communicate with the individual, or for other reasons, the CE must document the reason acknowledgment could not be obtained.

Refer to Chapter 12 for additional details.

Requests for restrictions

Individuals have the right to ask CEs to restrict:

- Uses and disclosures for treatment, payment, and operations;
- Disclosures to persons involved in the individual's care or payment for healthcare; and
- Disclosures to notify family members or others about the individual's general condition, location, or death.

Pursuant to HIPAA, individuals have the right to request these restrictions, but CEs are not required to agree to them. CEs that agree to restrictions must abide by them for as long as they remain effective.

NEW ARRA adds a new twist to restrictions. An individual may restrict a CE's ability to disclose information to health plans under HIPAA's payment and operations provisions. This restriction applies to services for which the individual pays out of pocket and in full.

Refer to Chapter 8 for more information on restrictions.

Special Uses and Disclosures

There are many uses for health information and just as many differing opinions as to who should be able to use it and for what purposes. In developing the Privacy Rule, HHS received input from a wide range of individuals and special interest groups regarding the use of PHI. The requirements described in the following section attempt to balance the needs of those groups with the individual's right to privacy.

Business associates

A business associate or BA is a person or organization (other than a member of the CE's workforce) that performs a function for the CE that requires access to PHI. BA functions include billing, claims processing, collections, data analysis, medical transcription, off-site record storage, and utilization review.

Persons or organizations are not considered BAs if their services don't involve use or disclosure of PHI or when access to PHI would be incidental, if at all.

The Privacy Rule requires certain protections for PHI used or disclosed by a BA. The CE and the BA must have a written contract that safeguards the information and restricts how the BA may use or disclose it.

NEW BAs that breathed a sigh of relief because they had limited obligations under HIPAA soon will see changes. Pursuant to ARRA, BAs must comply with selected privacy and security regulations. This includes the need for administrative, physical, and technical safeguards, as well as policies, procedures, and documentation requirements.

BAs also will be required to act on knowledge they may have concerning a CE's lack of compliance, and they will be subject to the tougher penalties prescribed by ARRA.

ARRA extends its breach notification requirements to BAs, requiring them to notify CEs if they experience any data breaches. CEs may also request that their BAs report the events themselves.

Refer to Chapter 6 for additional details.

De-identified data

If PHI is de-identified (that is, stripped of all identifiers that could link it to an individual), it may be freely used or disclosed. Information is considered de-identified if it is stripped of 18 specific identifiers or if a qualified statistician determines that the likelihood of linking it to an individual is extremely low.

Refer to Chapter 18 for additional details.

Fundraising

Providers may use limited patient information (generally, demographics and dates of service) for their fundraising activities. Any fundraising communications must identify the CE as the responsible party and tell individuals how they can opt out of future solicitations. CEs may not use information about diagnoses or procedures for targeted marketing to certain groups, such as cancer patients.

NEW ARRA addresses concerns with HIPAA's use of PHI for fundraising. The HHS secretary is directed to define the scope of fundraising activities that might be considered part of healthcare operations and how individuals must be informed of those activities.

Refer to Chapter 17 for more information on marketing and fundraising.

Limited data sets

The concept of limited data sets attempts to overcome the limitations of de-identified data (and many complaints from health services researchers). Limited data sets may be used only for research, public health, and healthcare operations.

In a limited data set, some identifiers may be kept with the data, including:

- Dates of admission, discharge, and other dates of service
- Date of birth

- Date of death
- Five-digit ZIP code

To protect information in a limited data set, there must be a written data use agreement between the CE and the individual or organization that will use the data.

NEW ARRA increases a CE's obligation to use a limited data set when responding to requests for PHI. If the limited data set does not meet the need for disclosure, an entity may make a determination of what constitutes "minimum necessary" for the disclosure. The HHS secretary is required to issue additional guidance in this area.

Refer to Chapter 18 for additional details.

Marketing

Marketing is defined as a communication that encourages the recipient to purchase or use a product or service. CEs must obtain written authorization from individuals or their personal representatives to use PHI for marketing purposes.

Certain activities that are not considered marketing include communications:

- To describe patient benefits
- For treatment of the patient
- For case management or care coordination
- That occur face-to-face
- Consisting of distribution of promotional items of nominal value, such as pens

NEW ARRA addresses concerns with HIPAA's use of PHI for marketing. It continues the prohibition of PHI use for marketing and calls for further regulation to define reasonable reimbursements for CEs and BAs.

Refer to Chapter 17 for more information.

Complaints and Incidents

Despite your best efforts—and, hopefully, those of your staff—some incidents will occur. Investigating and responding to complaints and incidents is an important part of your compliance program.

Pursuant to HIPAA, a CE must provide a process for individuals to file complaints about its privacy policies and procedures and must document all complaints received and their disposition. Incidents must also be documented and investigated even if no one files a complaint.

CEs must adopt and apply appropriate sanctions against workforce members who fail to comply with their privacy policies and procedures.

And when PHI is used or disclosed in violation of their policies, CEs must mitigate, to the extent practical, any harmful effects of which they are aware. This includes violations by their BAs.

NEW As the incidence and seriousness of privacy breaches have increased, so have demands from the public that more be done to protect their health information. In response, ARRA established the first federal requirements for health data breach reporting and notification. It extends those requirements beyond HIPAA's CEs to include BAs and non-CEs, such as vendors of PHRs.

Resources

1. Understanding and interpreting the regulations is an ever-evolving process, but the OCR helps by providing straightforward answers to questions submitted by the public. To access frequently asked questions on privacy issues with responses from the OCR, visit *www.hhs.gov/ocr/privacy*. Click on Answers to Your Frequently Asked Questions in the upper left section of the page.

2.. OCR also provides helpful privacy guidelines that explain specific aspects of the Privacy Rule in an easy-to-follow format with helpful examples. To access the privacy guidelines, visit *www.hhs.gov/ocr/privacy* and select Understanding HIPAA Privacy from the box on the left side of the page. Then select For Covered Entities and Guidance on Significant Aspects of the Privacy Rule.

3. To meet ARRA requirements, HHS also has established regional office privacy advisors. These advisors offer CEs, BAs, and individuals guidance and education with respect to their rights and responsibilities pertaining to federal privacy and security requirements for PHI. Refer to Figure 1.1 in the Appendix for contact information for regional office privacy advisors.

