DEPARTMENT OF HEALTH AND HUMAN SERVICES
Centers for Medicare & Medicaid Services

Medicare Learning Network®
Official Information Health Care Professionals Can Trust

Click Here to Open a Text-Only Version for Easy Printing

HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules were established to protect the privacy and security of health information and provide individuals with certain rights to their health information. Among other provisions, the Privacy Rule sets standards for when protected health information (PHI) may be used and disclosed, while the Security Rule requires safeguards to ensure only those who should have access to electronic protected health information (ePHI) will have access. The Breach Notification Rule requires HIPAA covered entities to notify the Department of Health & Human Services (HHS), affected individuals, and in some cases the media (and business associates to notify covered entities) of breaches of unsecured PHI.

Please note: The information in this publication applies to HIPAA covered entities, which include most Health Care Professionals and Health Care Organizations, as well as their business associates. When "you" is used in this publication, we are referring to these persons and entities.

ICN 909001 May 2015

You play a vital role in protecting the privacy and security of patient information. This fact sheet gives a basic overview of the rules, the information protected by the rules, and who must comply with the rules.

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes standards for the protection of PHI held by covered entities and their business associates (defined below) and gives patients important rights with respect to their health information. Additionally, the Privacy Rule permits the use and disclosure of health information needed for patient care and other important purposes.

Protected Information

The Privacy Rule protects individually identifiable health information, called PHI, held or transmitted by a covered entity or its business associate, in any form, whether electronic, paper, or verbal. PHI includes information that relates to the following:

- The individual's past, present, or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual.

PHI includes many common identifiers, such as name, address, birth date, and Social Security Number.

HIPAA Security Rule

The Security Rule specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of ePHI.

Implementation

Covered entities and business associates must develop and implement policies and procedures to protect the security of ePHI that they create, receive, maintain, or transmit. Each entity must analyze the risks to the ePHI in its environment and create solutions appropriate for its own situation. What is reasonable and appropriate for a particular entity will depend on the nature of the entity's business, as well as the entity's size, complexity, and resources. For more information on the implementation of the security standards, visit http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html on the HHS website.

HIPAA Breach Notification Rule

The Breach Notification Rule requires covered entities to notify affected individuals, HHS, and in some cases, the media of a breach of unsecured PHI. Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach. Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to HHS in a log or other documentation annually. The Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate. Table 1 displays the notification timelines.

Table 1. Breach Notification Timelines

Providing Notification To…	Breach Involved Fewer Than 500 Individuals	Breach Involved 500 or More Individuals
Individuals	No later than 60 days from discovery	No later than 60 days from discovery
HHS	Submit a log of all breaches once a year, no later than 60 days after end of calendar year	At same time as notice to individuals, no later than 60 days from discovery
Media	N/A	No later than 60 days from discovery

Who Must Comply With HIPAA Rules?

Covered entities and business associates must follow HIPAA rules. If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA rules. For a complete definition of a covered entity and a business associate, refer to http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf on the U.S. Government Publishing Office website.

Covered Entities

Covered entities electronically transmit health information. The following covered entities must follow HIPAA standards and requirements:

- **Covered Health Care Providers:** Any provider of medical or other health care services or supplies who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
- **Health Plans:** Any individual or group plan that provides or pays the cost of health care.
- **Health Care Clearinghouses:** A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice versa.

Business Associates

A business associate is a person or organization, other than an employee of a covered entity, that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI. A business associate can also be a subcontractor responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate.

If a covered entity enlists the help of a business associate, a written contract or other arrangement between the two must:

- Detail the uses and disclosures of PHI the business associate may make; and
- Require that the business associate safeguard the PHI.

What Are Covered Entities and Business Associates?

Covered Entities

Health Care Provider

This includes:

- Chiropractors;
- Clinics;
- Dentists;
- Doctors;
- Nursing homes;
- Pharmacies; and
- Psychologists.

Health Plan

This includes:

- Company health plans;
- Government programs that pay for health care, such as Medicare, Medicaid, along with the military and veterans' health care programs;
- Health insurance companies; and
- Health Maintenance Organizations.

Health Care Clearinghouse

This includes:

- Billing services;
- Community health management information systems;
- Repricing companies; and
- Value-added networks.

Business Associates

Business associates provide services to covered entities that include:

- Accreditation;
- Billing;
- Claims processing;
- Consulting;
- Data analysis;
- Financial services;
- Legal services;
- Management administration; and
- Utilization review.

NOTE: A covered entity can be a business associate of another covered entity.

Enforcement

The HHS Office for Civil Rights enforces the HIPAA Privacy, Security, and Breach Notification Rules. For more information on the enforcement process, visit http://www.hhs.gov/ocr/privacy/hipaa/enforcement on the HHS website. Violations may result in the imposition of civil monetary penalties. In some cases, criminal penalties may apply, enforced by the Department of Justice.

- **Case example of a settlement:** Two covered entities inadvertently posted ePHI for 6,800 individuals to the Internet, including patient status, vital signs, medications, and laboratory results. The investigation found that neither entity made efforts to assure the security of the server hosting the ePHI or confirm it contained adequate software protections. Neither entity developed an adequate risk management plan that addressed potential threats and hazards to ePHI. The entities agreed to pay a combined settlement of $4.8 million and enter into corrective action plans.
- **Case example of a criminal prosecution:** A former hospital employee pleaded guilty to criminal HIPAA charges after obtaining PHI with the intent to use it for personal gain. He faces up to 10 years in prison.

Resources

For more information about the HIPAA Privacy Rule and the HIPAA Security Rule, visit http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/PrivacyandSecurityStandards.html on the Centers for Medicare & Medicaid Services (CMS) website or scan the Quick Response (QR) code on the right.

Table 2. HIPAA Privacy, Security, and Breach Notification Resources

Resources	Website
Are You a Covered Entity?	http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html
Business Associate Contracts	http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
Business Associate Frequently Asked Questions	http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates
"Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care"	http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf
Disclosures in Emergency Situations	http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_in_emergency_situations

Table 2. HIPAA Privacy, Security, and Breach Notification Resources (cont.)

Resources	Website
Fast Facts for Covered Entities	http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/cefastfacts.html
"Frequently Asked Questions About the Disposal of Protected Health Information"	http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf
Model Notices of Privacy Practices	http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html
"Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification" Final Rule	http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
Security Risk Assessment	http://www.healthit.gov/providers-professionals/security-risk-assessment
Security Rule Guidance Material	http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
Training Materials	http://www.hhs.gov/ocr/privacy/hipaa/understanding/training
Your Mobile Device and Health Information Privacy and Security	http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

The Medicare Learning Network® Disclaimers are available at http://go.cms.gov/Disclaimer-MLN-Product on the CMS website.

The Medicare Learning Network® (MLN), a registered trademark of the U.S. Department of Health & Human Services (HHS), is the brand name for official information health care professionals can trust. For additional information, visit the MLN's web page at http://go.cms.gov/MLNGenInfo on the CMS website.

Your feedback is important to us and we use your suggestions to help us improve our educational products, services and activities and to develop products, services and activities that better meet your educational needs. To evaluate Medicare Learning Network® (MLN) products, services and activities you have participated in, received, or downloaded, please go to http://go.cms.gov/MLNProducts and in the left-hand menu click on the link called 'MLN Opinion Page' and follow the instructions. Please send your suggestions related to MLN product topics or formats to MLN@cms.hhs.gov.

Check out CMS on: