mln FACT SHEET
KNOWLEDGE • RESOURCES • TRAINING

PRINT-FRIENDLY VERSION

HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES

Target Audience: Medicare Fee-For-Service Providers

The Hyperlink Table, at the end of this document, provides the complete URL for each hyperlink.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and provide individuals with certain rights to their health information. You play a vital role in protecting the privacy and security of patient information. This fact sheet discusses:

- The **Privacy Rule**, which sets national standards for when protected health information (PHI) may be used and disclosed
- The **Security Rule**, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)
- The **Breach Notification Rule**, which requires covered entities to notify affected individuals; U.S. Department of Health & Human Services (HHS); and, in some cases, the media of a breach of unsecured PHI

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
Medicare Learning Network®

HIPAA PRIVACY RULE

The HIPAA Privacy Rule establishes standards to protect PHI held by these entities and their business associates:

- Health plans
- Health care clearinghouses
- Health care providers that conduct certain health care transactions electronically

When "you" is used in this fact sheet, we are referring to these entities and persons.

The Privacy Rule gives individuals important rights with respect to their protected PHI, including rights to examine and obtain a copy of their health records in the form and manner they request, and to ask for corrections to their information. Also, the Privacy Rule permits the use and disclosure of health information needed for patient care and other important purposes.

PHI

The Privacy Rule protects 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 all of the following:

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

Visit the HHS HIPAA Guidance webpage for guidance on:

- De-identifying PHI to meet HIPAA Privacy Rule requirements
- Individuals' right to access health information
- Permitted uses and disclosures of PHI

HIPAA SECURITY RULE

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

Covered entities and business associates must develop and implement reasonable and appropriate security measures through policies and procedures to protect the security of ePHI they create, receive, maintain, or transmit. Each entity must analyze the risks to ePHI in its environment and create solutions appropriate for its own situation. What is reasonable and appropriate depends on

the nature of the entity's business as well as its size, complexity, and resources. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the ePHI
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce

Confidentiality: ePHI is not available or disclosed to unauthorized persons or processes

Integrity: ePHI is not altered or destroyed in an unauthorized manner

Availability: ePHI is accessible and usable on demand by authorized persons

When developing and implementing Security Rule compliant safeguards, covered entities and their business associates may consider all of the following:

- Size, complexity, and capabilities
- Technical, hardware, and software infrastructure
- The costs of security measures
- The likelihood and possible impact of risks to ePHI

Covered entities must review and modify security measures to continue protecting ePHI in a changing environment.

Visit the HHS HIPAA Guidance webpage for guidance on:

- Administrative, physical, and technical safeguards
- Cybersecurity
- Remote and mobile use of ePHI

HIPAA BREACH NOTIFICATION RULE

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals; HHS; and, in some cases, the media of a breach of unsecured PHI. Generally, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. The impermissible use or disclosure of PHI is presumed to be a breach unless you demonstrate there is a low probability the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made

- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated.

Most notifications must be provided without unreasonable delay and no later than 60 days following the breach discovery. Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to HHS annually. The Breach Notification Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.

Visit the HHS HIPAA Breach Notification Rule webpage for guidance on:

- Administrative requirements and burden of proof
- How to make unsecured PHI unusable, unreadable, or indecipherable to unauthorized individuals
- Reporting requirements

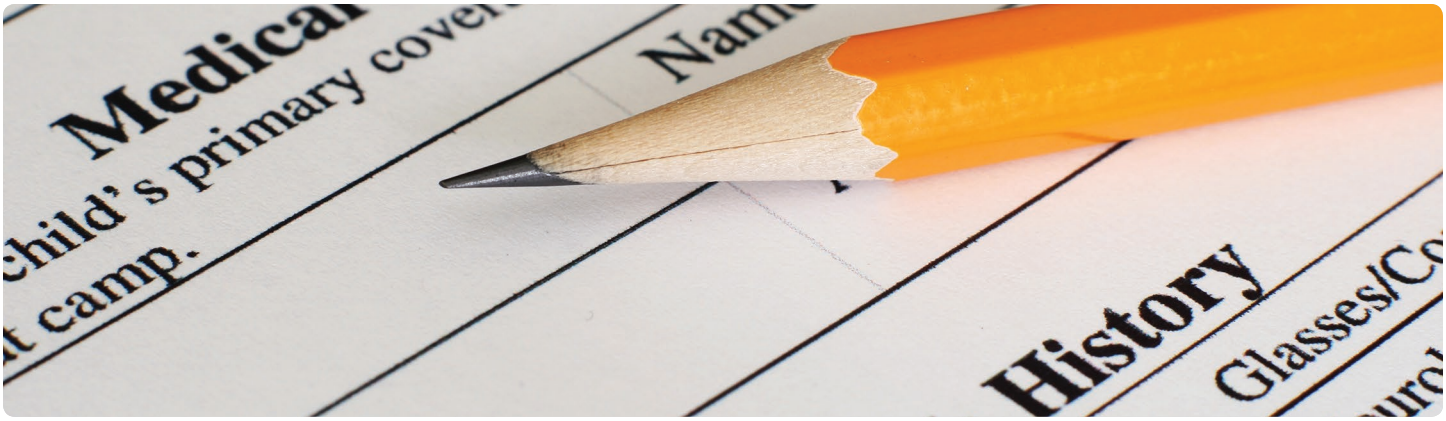
WHO MUST COMPLY WITH HIPAA RULES?

Covered entities and business associates, as applicable, 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 the definitions of "covered entity" and "business associate," see the Code of Federal Regulations (CFR) Title 45, Section 160.103.

Covered Entities

The following covered entities must follow HIPAA standards and requirements:

- **Covered Health Care Provider:** 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, such as:
  - Chiropractors
  - Clinics
  - Dentists
  - Doctors
  - Nursing homes
  - Pharmacies
  - Psychologists
- **Health Plan:** Any individual or group plan that provides or pays the cost of health care, such as:
  - Company health plans
  - Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs
  - Health insurance companies
  - Health maintenance organizations (HMOs)



- **Health Care Clearinghouse:** 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, such as:
  - Billing services
  - Community health management information systems
  - Repricing companies
  - Value-added networks

Business Associates

A business associate is a person or organization, other than a workforce member 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. Business associates provide services to covered entities that include:

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

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

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

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

Visit the HHS HIPAA Covered Entities and Business Associates webpage for more information.

Enforcement

The HHS Office for Civil Rights enforces the HIPAA Privacy, Security, and Breach Notification Rules. Violations may result in civil monetary penalties. In some cases, criminal penalties enforced by the U.S. Department of Justice may apply.

Common violations include:

- Impermissible PHI use and disclosure
- Use or disclosure of more than the minimum necessary PHI
- Lack of PHI safeguards
- Lack of administrative, technical, or physical ePHI safeguards
- Lack of individuals' access to their PHI

The following are actual case examples:

- **HIPAA Privacy and Security Rule:** A wireless health service provider (remote mobile monitoring) agreed to pay $2.5 million and implement a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. A laptop with 1,391 individuals' ePHI was stolen from an employee's vehicle. The investigation revealed insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, the organization's policies and procedures implementing HIPAA Security Rule standards were in draft form and had not been implemented. Further, the organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.
- **HIPAA Breach Notification Rule:** A specialty clinic agreed to pay $150,000 to settle potential violations of the HIPAA rules. An unencrypted thumb drive with the ePHI of about 2,200 individuals was stolen from a clinic employee's vehicle. The investigation revealed the clinic had not accurately or thoroughly analyzed the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, the clinic did not fully comply with requirements of the Breach Notification Rule to have written policies and procedures in place and train workforce members. This case was the first settlement with a covered entity for not having policies and procedures to address the HIPAA Breach Notification Rule.
- **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 was sentenced to 18 months in Federal prison.

Visit the HHS HIPAA Compliance and Enforcement webpage for more information.

Resources

Refer to the HHS Special Topics in Health Information Privacy webpage for information on:

- Cloud computing
- Mobile apps
- HIPAA regulation history

Table 1. HIPAA Privacy, Security, and Breach Notification Resources

For More Information About…	Resource
Covered Entities	Covered Entity Guidance CMS.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf Fast Facts HHS.gov/hipaa/for-professionals/covered-entities/fast-facts
Business Associates	Contracts HHS.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions Frequently Asked Questions HHS.gov/hipaa/for-professionals/faq/business-associates
Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care	HHS.gov/sites/default/files/provider_ffg.pdf HHS.gov/hipaa/for-professionals/special-topics/mental-health
Emergency Situations: Preparedness, Planning, and Response	HHS.gov/hipaa/for-professionals/special-topics/emergency-preparedness
PHI Disposal	HHS.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf
Privacy and Security of Electronic Health Records (EHR)	HealthIT.gov/topic/privacy-security-and-hipaa
Model Notices of Privacy Practices	HHS.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices

Table 1. HIPAA Privacy, Security, and Breach Notification Resources (cont.)

For More Information About…	Resource
Omnibus HIPAA Final Rule (2013 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules)	GPO.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
Security Rule Guidance Material	HHS.gov/hipaa/for-professionals/security/guidance
Training Materials	HHS.gov/hipaa/for-professionals/training

Table 2. Hyperlink Table

Embedded Hyperlink	Complete URL
Code of Federal Regulations (CFR) Title 45, Section 160.103	https://www.ecfr.gov/cgi-bin/text-idx?SID=2e74ee451fc72a29cdf7e67af5219ce6&mc=true&node=pt45.1.160&rgn=div5#se45.1.160_1103
HHS Special Topics in Health Information Privacy	https://www.hhs.gov/hipaa/for-professionals/special-topics
HIPAA Breach Notification Rule	https://www.hhs.gov/hipaa/for-professionals/breach-notification
HIPAA Compliance and Enforcement	https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement
HIPAA Covered Entities and Business Associates	https://www.hhs.gov/hipaa/for-professionals/covered-entities
HIPAA Guidance	https://www.hhs.gov/hipaa/for-professionals/privacy/guidance