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

What's Changed?

- Added Information – Privacy Rule protections and rights, page 3
- Added Information – Keeping PHI private and confidential, page 4
- Added Information – Sharing information with other health care professionals, page 4
- Added Information – Sharing patient information with family members and others, page 4
- Added Information – Incidental disclosures, page 5
- Added Information – Protecting and securing health information when using a mobile device, page 5

You'll find substantive content updates in dark red font.

Table of Contents

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and gives individuals rights to their health information. HIPAA 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 see "you" in this booklet, we're referring to these covered entities and persons.

This booklet discusses:

- The **Privacy Rule**, which sets national standards for the use and disclosure of protected health information (PHI)
- The **Security Rule**, which specifies safeguards that covered entities and their business associates must use 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, HHS, and, in some cases, the media of a breach of unsecured PHI

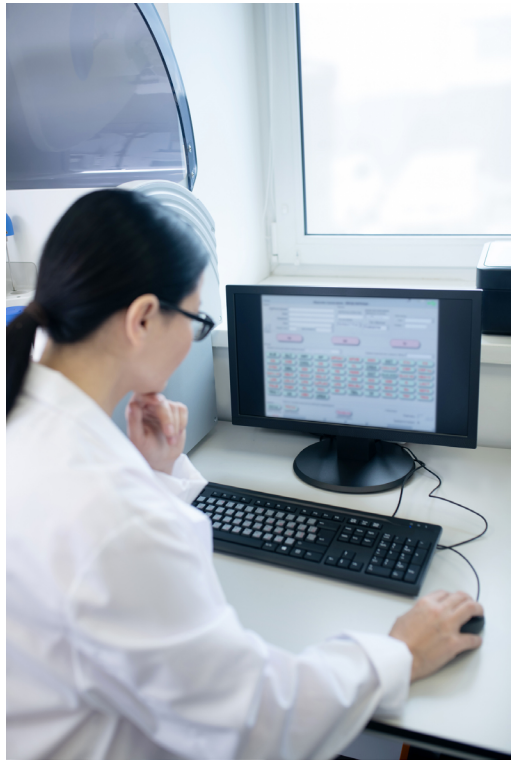
HIPAA Privacy Rule

The Privacy Rule protects your patients' PHI while letting you exchange information to coordinate your patient's care. The Privacy Rule also gives patients the right to examine and get a copy of their medical records, including an electronic copy of their electronic medical records, and to request corrections. Under the Privacy Rule, patients can restrict their health plan's access to information about treatments they paid for in cash, and most health plans can't use or disclose genetic information for underwriting purposes. The Privacy Rule allows you to report child abuse or neglect to the authorities.

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 about:

- Common identifiers, such as name, address, birth date, and Social Security number
- 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



Keeping PHI Private & Confidential

The Privacy Rule requires you to:

- Notify patients about their privacy rights and how you use their information
- Adopt privacy procedures and train employees to follow them
- Assign an individual to make sure you're adopting and following privacy procedures
- Secure patient records containing PHI so they aren't readily available to those who don't need to see them

Sharing Information with Other Health Care Professionals

To coordinate your patient's care with other providers, the Privacy Rule lets you:

- Share information with doctors, hospitals, and ambulances for treatment, payment, and health care operations, even without a signed consent form from the patient
- Share information about an incapacitated patient if you believe it's in your patient's best interest
- Use health information for research purposes
- Use email, telephone, or fax machines to communicate with other health care professionals and with patients, as long as you use safeguards

Sharing Patient Information with Family Members & Others

Unless a patient objects, the Privacy Rule lets you:

- Give information to a patient's family, friends, or anyone else identified by the patient as involved in their care

- Give information about the patient's general condition or location to a patient's family member or anyone responsible for the patient's care
- Include basic information in a hospital directory, such as the patient's phone and room number
- Give information about a patient's religious affiliation to members of the clergy

Incidental Disclosures

The HIPAA Privacy Rule requires you to have policies that protect and limit how you use and disclose PHI, but you aren't expected to guarantee the privacy of PHI against all risks. Sometimes, you can't reasonably prevent limited disclosures, even when you're following HIPAA requirements. For example, a hospital visitor may overhear a doctor's confidential conversation with a nurse or glimpse a patient's information on a sign-in sheet. These incidental disclosures aren't considered a HIPAA violation as long as you're following the required reasonable safeguards.

The Office for Civil Rights (OCR) offers guidance about how this applies to health care practices, including an Incidental Uses and Disclosures subcategory in its FAQs.

Securing Health Information When Using a Mobile Device

- Use a password or other user authentication
- Install and enable encryption
- Install and activate remote wiping or remote disabling
- Disable and don't install or use file sharing applications
- Install and enable a firewall
- Install and enable security software
- Keep your security software up to date
- Research mobile applications (apps) before downloading
- Maintain physical control
- Use adequate security to send or receive health information over public Wi-Fi networks
- Delete all stored health information before discarding or reusing the mobile device

Visit the HHS HIPAA Guidance Materials webpage for information about:

- 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 includes security requirements to protect patients' ePHI confidentiality, integrity, and availability. The Security Rule requires you to develop reasonable and appropriate security policies. In addition, you must analyze security risks in your environment and create appropriate solutions. What's reasonable and appropriate depends on your business as well as its size, complexity, and resources. You should always review and modify security measures to continue protecting ePHI in a changing environment.

Specifically, you must:

- Ensure the confidentiality, integrity, and availability of all ePHI you create, receive, maintain, or transmit
- Identify and protect against threats to ePHI security or integrity
- Protect against impermissible uses or disclosures
- Ensure employee compliance

When developing compliant safety measures, consider:

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

Confidentiality: ePHI can't be available or disclosed to unauthorized persons or processes

Integrity: ePHI can't be altered or destroyed in an unauthorized manner

Availability: ePHI has to be accessible and usable on demand by authorized persons

Visit the HHS HIPAA Guidance Materials webpage for guidance on:

- Administrative, physical, and technical PHI safety measures
- Cybersecurity
- Remote and mobile use of ePHI

HIPAA Breach Notification Rule

When you experience a PHI breach, the HIPAA Breach Notification Rule requires you to notify affected individuals, HHS, and, in some cases, the media. Generally, a breach is an unpermitted use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. The unpermitted use or disclosure of PHI is a breach unless there is a low probability the PHI has been compromised, based on a risk assessment of:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or received the disclosed PHI
- Whether an individual acquired or viewed the PHI
- The extent to which you reduced the PHI risk

You must notify authorities of most breaches without reasonable delay and no later than 60 days after discovering the breach. Submit notifications of smaller breaches affecting fewer than 500 individuals to HHS annually. The Breach Notification Rule also requires business associates to notify a 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 must follow HIPAA rules. If you don't meet the definition of a covered entity or business associate, you don't have to comply with the HIPAA rules.

For definitions of covered entity and business associate, see the Code of Federal Regulations (CFR) Title 45, Section 160.103.

Covered Entities

Covered entities that must follow HIPAA standards and requirements include:

- **Covered Health Care Provider:** Any provider of medical or other health care services or supplies that transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard, such as:
  - Doctors
  - Clinics
  - Psychologists
  - Dentists
  - Chiropractors
  - Nursing Homes
  - Pharmacies
- **Health Plan:** Any individual or group plan that provides or pays the cost of health care, such as:
  - Health insurance companies
  - Health maintenance organizations
  - Company health plans
  - Government programs that pay for health care
- **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 functions on behalf of or provides services to a covered entity that involve PHI access. Business associates also include subcontractors 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 you work with a business associate, a written contract or other arrangement between you must:

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

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

Enforcement

The HHS Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules.

Violations may result in civil monetary penalties. In some cases, U.S. Department of Justice enforced criminal penalties may apply. Common violations include:

- Unpermitted 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 agreed to pay $2.5 million to settle potential violations of the HIPAA Privacy and Security Rules after someone stole a laptop with 1,391 individuals' ePHI from an employee's vehicle. The investigation revealed insufficient risk analysis and management processes at the time of the theft. Additionally, the organization's HIPAA Security Rule policies and procedures were in draft form. The organization couldn't produce any final policies or procedures regarding safeguards for ePHI, including 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 hadn't accurately or thoroughly analyzed the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. The clinic also didn't comply with Breach Notification Rule requirements for written policies and procedures and employee training. 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 intending to use it for personal gain. He was sentenced to 18 months in federal prison.

Find more information on the HHS HIPAA Enforcement webpage.

Resources

- Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care and Model Notices of Privacy Practices
- FAQs about the Disposal of Protected Health Information
- Business Associate Contracts and Business Associates FAQs
- Fast Facts for Covered Entities and Covered Entity Guidance
- HIPAA FAQs for Professionals
- Omnibus HIPAA Final Rule (2013 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules)
- Privacy, Security, and HIPAA
- Security Rule Guidance Material
- Training Materials
- Special Topics in Health Information Privacy