mln Fact Sheet
KNOWLEDGE • RESOURCES • TRAINING

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

**What's Changed?**

Note: No substantive content updates



CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
Medicare Learning Network®

## Health Insurance Portability & Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and give patients' rights to their health information. HIPAA establishes standards to protect people's medical records and other protected health information (PHI). These standards apply to the following covered entities and their business associates:

- Health plan
- Health care clearinghouse
- Health care provider that conducts certain health care transactions electronically

## Privacy Rule

The Privacy Rule protects your patients' PHI while letting you securely exchange information to coordinate your patients' care. The Privacy Rule also gives patients the right to:

- Examine and get a copy of their medical records, including an electronic copy
- Request corrections to their medical records
- Restrict their health plan's access to information about treatments they paid for in cash

Under the Privacy Rule, most health plans can't use or disclose genetic information for underwriting purpose.

You can report child abuse or neglect to the authorities.

### PHI

The Privacy Rule protects PHI that you hold or transmit in any form, including electronic, paper, or verbal. PHI includes information about:

- Personal identifiers, like name, address, birth date, and SSN
- Past, present, or future physical or mental health condition
- Health care you provide to the patient
- The past, present, or future payment for health care you provide to the patient

## Requirements

Under the Privacy Rule, you must:

- Notify patients about their privacy rights and how you use their information
- Adopt privacy procedures and train employees to follow them
- Assign employee 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, you can:

- 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, phone, 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, you can:

- Give information to a patient's family, friends, or anyone else the patient identifies 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, like the patient's phone and room number
- Give information about a patient's religious affiliation to clergy members

## Incidental Disclosures

You must have policies that protect PHI and limit how you use and share it. But you don't have to guarantee complete privacy in every situation Sometimes, you can't reasonably prevent limited disclosures, even when you're following HIPAA requirements.

For example, a hospital visitor might overhear a private conversation between a doctor and a nurse or see a patient's name on a sign-in sheet. These accidental disclosures aren't HIPAA violations if you take steps to protect patient privacy whenever you can.

The Office for Civil Rights (OCR) offers guidance about how this applies to health care practices, including incidental uses and disclosures FAQs.

Visit HHS HIPAA Guidance Materials for information about:

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

## Security Rule

The Security Rule includes security requirements to protect patients' electronic PHI (ePHI) confidentiality, integrity, and availability. The Security Rule requires you to:

- Develop reasonable and appropriate security policies
- 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
- Analyze security risks in your environment and create appropriate solutions
- Review and modify security measures to continue protecting ePHI in a changing environment
- 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 of risk and how they might affect ePHI

Visit HHS Cyber Security Guidance Material for information about:

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

## Breach Notification Rule

You must follow the Breach Notification Rule if a breach involves PHI. That means you must notify affected patients, HHS, and, in some cases, the media. A breach usually happens when PHI is used or shared in a way that isn't allowed under the HIPAA Privacy Rule – and that use or disclosure puts the privacy or security of the information at risk. Any use or disclosure of PHI that isn't permitted is considered a breach unless there's a low probability the PHI has been compromised, based on a risk assessment of:

- The type of PHI involved, including what identifiers and the chances someone could identify the patient
- Who used the PHI or got the PHI without permission
- Whether anyone viewed or kept the PHI
- What steps you took to reduce the risk after the incident

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 patients to HHS annually. The Breach Notification Rule also requires your business associates to notify you of breaches at or by the business associate.

Visit the HHS Breach Notification Rule for information about:

- 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.

Learn more about covered entities and business associates, including fast facts for covered entities.

For definitions of covered entities and business associates, see 45 CFR 160.103.

## Who Enforces HIPAA Rules?

The HHS 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
- Not giving patients' access to their PHI

For more information, including case examples, visit the HHS HIPAA Enforcement webpage.

## Resources

- HIPAA FAQs for Professionals
- Model Notices of Privacy Practices
- Privacy, Security, and HIPAA
- Special Topics in Health Information Privacy
- Training Materials

View the Medicare Learning Network® Content Disclaimer and Department of Health & Human Services Disclosure