HIPAA Rules: Privacy, Security and Electronic Data Interchange

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a broad federal law regarding health coverage. It contains provisions related to the portability of health coverage and provisions prohibiting discrimination based upon an individual's health status. HIPAA also includes administrative simplification provisions. HIPAA's administrative simplification provisions relate to:

- Ensuring the **privacy and security** of personally identifiable health information (the Privacy and Security Rules); and
- Setting **uniform standards for electronic health care transactions** (Electronic Data Interchange or EDI Rules).

HIPAA's administrative simplification rules generally apply to health care providers, health plans and healthcare clearinghouses ("covered entities"). Certain requirements also apply to entities—called "business associates"—that perform functions on behalf of covered entities involving protected health information (PHI).

LINKS AND RESOURCES

The U.S. Department of Health and Human Services (HHS) oversees HIPAA's Privacy, Security and EDI Rules. Click on the following links for more information:

- The HIPAA Privacy Rule
- The HIPAA Security Rule
- Information on HIPAA compliance and enforcement

HIPAA Rules

- The Privacy Rule governs the use and disclosure of protected health information (or PHI).
- The Security Rule requires covered entities and business associates to safeguard electronic PHI (or ePHI).
- The EDI Rule requires covered entities to keep and exchange information in a uniform format.

Affected Entities

- The HIPAA Rules apply to covered entities and business associates.
- A "covered entity" is a health plan, a health care clearinghouse or a health care provider that conducts certain transactions electronically.
- In general, a business associate is an entity that performs a function, activity or specific service for a covered entity that involves PHI.

Privacy Rule

The HIPAA Privacy Rule governs the use and disclosure of personally identifiable health information. Key provisions of the Privacy Rule are listed below.

Key Provision	Description

Key Provision	Description
Protected information	The Privacy Rule governs protected health information, or PHI, which is individually identifiable health information in any form (oral, paper and electronic). To qualify as PHI, the information must be created or received by a covered entity and it must relate to: The past, present or future physical or mental health or condition of an individual; The provision of health care to an individual; or The past, present or future payment for the provision of health care to an individual. PHI does not include employment records held by an employer in its role as an employer (not a plan administrator).
Covered entities	The main organizations governed by HIPAA's Privacy, Security and EDI Rules are known as covered entities, which include health plans, health care clearinghouses and health care providers that conduct certain financial and administrative transactions electronically. Self-administered, self-funded group health plans with fewer than 50 plan participants are exempt.
Individual Rights	Health plan participants must be given detailed written information that explains their privacy rights and how their information will be used (a Notice of Privacy Practices). Participants have a right to access their own health records and request corrections. Participants also have the right to request restrictions on the use and disclosure of their PHI, to obtain documentation of certain disclosures made about their health care records and to request that they receive their PHI at alternative locations or by alternative means.
Permitted uses and disclosures	The Privacy Rule provides that PHI may not be used or disclosed other than as permitted by the Privacy Rule. The main permitted uses are for treatment of the individual, payment for the individual's health care and health care operations of the covered entity. PHI may also be disclosed to plan sponsors for purposes of plan administrative activities. In some cases, disclosures may be made to an individual's family and/or friends and for specific public policy purposes. Specific authorization must be obtained prior to any disclosure that is not expressly permitted by the Privacy Rule. Employers that sponsor health plans may not gain access to health information for employment-related purposes without the participant's written HIPAA authorization.
Business associates	Covered entities may disclose PHI to certain vendors or service providers, known as business associates, if a proper contract protecting the PHI is in place. Business associates are also required by law to comply with some provisions of the Privacy Rule.
Minimum necessary standard	In general, when a covered entity uses, discloses or requests PHI, it must limit its use, disclosure or request to the minimum necessary amount of information to accomplish the intended purpose. Disclosures for treatment purposes and requests made by the patient for information regarding his or her own medical records are not subject to the minimum necessary standard.
Administrative requirements	Covered entities must comply with certain administrative requirements, such as appointing a privacy official, implementing safeguards to protect PHI and training members of the workforce. There is an exception for fully insured plans that do not receive PHI from the health insurance carrier. These plans are not required to comply with the Privacy Rule's administrative requirements, including the requirement to maintain and distribute a Notice of Privacy Practices to plan participants.
State privacy laws	Where a state has passed a law that conflicts with the Privacy Rule, the law that provides the greater privacy protections applies.

Security Rule

The HIPAA Security Rule imposes requirements on covered entities with respect to the protection of **electronic PHI (ePHI)**. Key aspects of the Security Rule are as follows:

Key Provision	Description
Safeguarding ePHI	The main purpose of the Security Rule is to ensure the confidentiality, availability and integrity of ePHI. Covered entities must protect against reasonably anticipated threats to ePHI and uses or disclosures of ePHI that are not permitted under the Privacy Rule. Covered Entities must also protect ePHI by ensuring that their workforces comply with the security requirements.
Security standards	Covered entities must implement reasonable and appropriate security standards to protect ePHI. The standards are intended to be flexible depending on the type, size and capabilities of the covered entity. There are specific standards for administrative, technical and physical safeguards. Covered entities should periodically review their security standards and make any necessary updates to their safeguards.
Business associates	If a covered entity uses a business associate, the contract between the two parties should address both privacy and security requirements for all types of PHI, including ePHI. Business Associates are also directly subject to many Security Rule requirements and should have their own security measures in place to safeguard ePHI.

Electronic Data Interchange Rule

The EDI Rule is intended to streamline electronic health care transactions by requiring that covered entities keep and exchange information in a uniform format. Key aspects of the EDI Rule are as follows:

Key Provision	Description
Standardized transactions	The EDI Rule provides that, if a covered entity (or a business associate on its behalf) electronically conducts a covered transaction, then the entity must use standardized formats and uniform codes when conducting the transaction.
Covered electronic transactions	The following transactions are governed by the EDI Rule: health care claims or equivalent encounter information; health care payment and remittance advice; coordination of benefits; health care claim status; enrollment and disenrollment in a health plan; eligibility for a health plan; health plan premium payments; and referral certification and authorization. The Affordable Care Act (ACA) added the following transactions to the list of covered electronic transactions—electronic funds transfers and health claims attachments.

HIPAA Enforcement

The Office of Civil Rights (OCR), a division of HHS, is responsible for the enforcement of HIPAA's Privacy and Security Rules. Key enforcement provisions are as follows:

Key Provision	Description
Civil enforcement	The OCR may assess civil penalties for HIPAA violations. These penalties may not apply if the violation is corrected within 30 days of the date the person knew, or should have known, of the violation. Rather than imposing civil penalties, OCR often resolves HIPAA violations informally with covered entities (or business associates) through resolution agreements. These agreements typically include a monetary settlement amount that is a fraction of the potential civil monetary penalties and a corrective action plan that requires the covered entity (or business associate) to fix remaining compliance issues.
Criminal enforcement	The potential criminal penalties vary depending on the circumstances of the violation: $50,000 and/or one year in prison for knowingly obtaining or disclosing protected information; $100,000 and/or up to five years in prison for obtaining information under false pretenses; and $250,000 and/or up to ten years in prison for obtaining PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.
HIPAA Audits	HHS is required to conduct periodic audits to ensure that covered entities and business associates are complying with the HIPAA Rules. In December 2020, HHS released its 2016-2017 HIPAA Audits Industry Report that reviewed selected covered entities and business associates for HIPAA compliance. According to a HIPAA enforcement report for 2021, OCR did not perform any audits during 2021 due to a lack of financial resources.