HIPAA INFORMATION

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule

How It Came About

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form.

The HIPAA Privacy Rule, in effect since 2001, establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections. The rule applies to Covered Entities and their business associates (subcontractors, providers and the like).

What the Rule Does

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.
- For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.
- It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
- It empowers individuals to control certain uses and disclosures of their health information.

What Information Is Protected

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's computer system
- Billing information about you at your clinic
- Most other health information about you held by those who must follow these laws

Covered Entities

Under the HIPAA Privacy Rule, Covered Entities and their business associates must guard against the misuse of an individual's identifiable health information and limit the sharing of such information.

Covered Entities include, but are not limited to, the following:

- Health Care Provider (hospitals, doctors, dentists, psychologists, clinics, pharmacies, nursing homes, and laboratories)
- Health Plans (via health insurance or self-insurance) Dental Plans (via health insurance or self-insurance) Vision Providers (via health insurance or self-insurance)
- Employee Assistance Plans that provide health benefits (via health insurance or self-insurance)
- Health insurance providers
- PPOs, HMOs, and managed health care organizations
- Health Care Spending or Reimbursement Accounts (flexible spending accounts under a cafeteria plan)
- Medical billing services
- Health Care Clearinghouse

Who Is Not Required to Follow the Rule

Examples of organizations that do not have to follow the Privacy and Security Rules include:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

Your Rights Over Your Health Information

Health insurers and providers who are covered entities must comply with your right to:

- Ask to see and get a copy of your health records
- Have corrections added to your health information
- Receive a notice that tells you how your health information may be used and shared
- Decide if you want to give your permission before your health information can be used or shared for certain purposes, such as for marketing
- Get a report on when and why your health information was shared for certain purposes
- If you believe your rights are being denied or your health information isn't being protected, you can:
  - File a complaint with your provider or health insurer
  - File a complaint with HHS

You should get to know these important rights, which help you protect your health information.

You can ask your provider or health insurer questions about your rights.

Who Can Look at and Receive Your Health Information

The Privacy Rule sets rules and limits on who can look at and receive your health information.

To make sure that your health information is protected in a way that does not interfere with your health care, your information can be used and shared:

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and to help run their businesses
- With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot:

- Give your information to your employer
- Use or share your information for marketing or advertising purposes or sell your information

HIPAA Security Rule

What Is It?

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Secretary of HHS to publish national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information.

HIPAA called on the Secretary to issue security regulations regarding measures for protecting the integrity, confidentiality, and availability of e-PHI that is held or transmitted by covered entities. HHS developed a proposed rule and released it for public comment on August 12, 1998. The final regulation, the Security Rule, was published February 20, 2003.

Who's Covered by the Security Rule?

The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates. The HITECH Act of 2009 expanded the responsibilities of business associates under the HIPAA Security Rule. Any telehealth providers also need to meet HIPAA Security Rule regulations.

What Information Is Protected?

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

General Rules

The Security Rule requires covered entities and their business associates to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

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

The Security Rule defines "confidentiality" to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, "integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. "Availability" means that e-PHI is accessible and usable on demand by an authorized person.

For More Information

TINYURL.COM/FD-HIPAA

Visit tinyurl.com/FD-HIPAA or scan this QR code for more information on the Health Insurance Portability and Accountability Act (HIPAA), including:

- Anti-Discrimination Notice
- Breach Notification
- HIPAA and the Definition of Spouse and Family
- Mental Health
- Protected Health Information (PHI)
- Statement of HIPAA Portability Rights

Item# Y5179526-U Y5179527-L FD-HIPAA+D 0423