irwin siegel agency
INSURANCE PROGRAMS & RISK MANAGEMENT

10 THINGS TO KNOW ABOUT HIPAA

CONTENTS

10 THINGS TO KNOW ABOUT HIPAA

1 WHAT IS HIPAA AND WHERE DID IT COME FROM?

The Health Insurance Portability and Accountability Act (HIPAA) became a federal law in 1996. HIPAA came about in response to several emerging issues due to continuing technological advances in the country's healthcare system. Put simply, it provides portability of healthcare coverage when employees change jobs, protects healthcare data integrity, confidentiality, and availability, and reduces fraud and abuse in the Medicare and Medicaid systems. The law required the establishment of privacy and security standards. The Privacy Rule governs the use and disclosure of Protected Health Information (PHI), including any personal and identifiable information related to an individual's health record, and the Security Rule establishes requirements for technological safeguards in the storing and transmitting that data in electronic format. The Act aims to protect individuals' health information while allowing for appropriate communication needed to provide and promote high-quality health care.

2 WHAT IS COVERED UNDER THE HIPAA PRIVACY RULE?

The Privacy Rule regulates how certain entities, called covered entities, may use and disclose protected health information, including past, present and future mental or physical health, and payment for care. To be covered under HIPAA, health information kept by a covered entity, usually a health care provider, health care plan, or health care clearinghouse, or a business entity doing business with a covered entity, combined with some fact that identifies an individual (such as a name, address, telephone number, Social Security number) is called "protected health information" or PHI. PHI can be oral, handwritten, or in an electronic format. This means a conversation between a doctor and nurse about your condition has the same general protections as information written on your records.

Each covered entity is also required to provide a notice of its privacy practices describing the ways it may use and disclose PHI. It must also inform the individual of his/her rights as established under the Act, including the right to file a complaint to HHS if it is believed that privacy rights have been violated. There must also be an individual point of contact identified for obtaining further information or to file a complaint.

3

WHO IS COVERED UNDER HIPAA?

HIPAA pertains to three categories of "covered entities" - health care providers, health plans, and health care clearinghouses. It also pertains to entities (called Business Associates) engaged in doing business with a covered entity such as a physicians' billing service.

- **Health Care Providers** are covered if they transmit health information electronically, even a doctor in a small practice with paper records who uses a billing service that transmits information electronically. Because the provider is engaged in doing business with an entity which provides for electronic format and transmission they would be covered under HIPAA. In short it is nearly impossible to provide health care today without using electronic means in some way.

  If any identifiable information is transmitted electronically a "health care provider" includes doctors, hospitals, staff involved in providing treatment, laboratories, pharmacists, dentists, and many others that provide medical, dental, and mental health care or treatment. In short, a provider is almost anyone in the business of providing health care who is licensed or regulated by the states.

HIPAA SCENARIO

A nurse discussed testing procedures with an individual in the waiting room of his doctor's office, disclosing PHI to several other individuals. The provider was mandated to develop and implement policies and procedures regarding appropriate administrative safeguards related to the communication of PHI.

- **Health Plan** means an entity that processes claims and/or provides payment for services covered under the Act. This includes: health insurance companies, HMOs (health maintenance organizations), group health plans sponsored by your employer, Medicare and Medicaid, and virtually any other company or arrangement that provides payment for health care related services.

- **Healthcare Clearinghouses** can be any number of organizations that work as a go-between for health care providers and health plans. An example of this would be a billing service that takes information from a doctor and puts it into a standard coded format. Patients rarely deal directly with clearinghouses.

- **Business Associates** include any person or organization that performs activities which involve disclosure of PHI on behalf of or for a covered entity such as claims processing, data analysis, quality assurance, billing, benefit management, financial services or accreditation.

4 WHAT DOES PHI INCLUDE?

PHI includes any information, oral or recorded in any form or medium, that is created or received by a health care provider and relates to past, present or future physical or mental health or condition of an individual, including the provision of care and payment for services.

Examples of PHI include:

- ☑ Name
- ☑ Address
- ☑ Birth Date
- ☑ Admission or Discharge Dates
- ☑ Date of Death
- ☑ Telephone or Fax Numbers
- ☑ Email Address
- ☑ Social Security Numbers
- ☑ Medical Records Numbers
- ☑ Health Plan Beneficiary Number
- ☑ Account Numbers
- ☑ Medical Record/Chart
- ☑ Emotional Support Animals
- ☑ Photographs

HIPAA SCENARIO

A direct care staff informed a consumer about his medication change in the living room in front of other consumers. The staff member was reported to management and the disclosure of PHI was reported to the Privacy Officer. The staff was re-trained on HIPAA Privacy Laws and the agency's policy regarding sharing information.

Disposal

Any covered entities must ensure that all of their workers receive training on and follow the disposal policies and procedures even if they are not involved directly. Entities are not permitted to abandon or dispose of PHI in any containers that may be accessible to the public or unauthorized person.

Examples of proper disposal:

- Paper Records: Shredding, burning, pulping, or pulverizing.
- Labeled Prescriptions Bottles/Other PHI in opaque bags: Using a disposal vendor to pick up and shred or destroy the PHI. You can also connect with a local drug take back site to safety dispose of any medicine.
- Electronic Media: clearing with software, purging, or destroying the media.

5 WHO HAS THE RIGHT TO ACCESS INFORMATION?

Individuals have the right to access their own health information. In some cases, personal representatives of the individuals, including parents of minors and legal guardians, may have the right to access PHI. Under HIPAA, patients can request a copy of their medical records from their health care provider. This typically requires completing release paperwork and may require a printing or copying fee. In some circumstances, availability of certain records may be limited.

6

WHAT RIGHTS DO I HAVE CONCERNING MY PROTECTED HEALTH INFORMATION?

You have the following rights (A through E) with respect to your protected health information:

A. The Right to Request Limits on Uses and Disclosures of Your Health Information. You have the right to limit how your health information is used and disclosed. Please note that you are not permitted to limit the uses and disclosures that are required or allowed by law to make.

B. The Right to Choose How Health Information is Sent to You or How You are Contacted. You have the right to ask that you are contacted at an alternate address or telephone number (for example, sending information to your work address instead of your home address) or by alternate means.

C. The Right to See or to Get a Copy of Your Protected Health Information. In most cases, you have the right to look at or get a copy of your health information, but you must make the request in writing. In certain situations, requests may denied. All denied requests will be explained, in writing. You have a right to appeal the decision.

If you request a copy of any portion of your protected ealth information, there will be a charge for the copy on a per page basis. It is required that payment be made in full before the copy is provided. If agreed in advance, a summary or an explanation of your records can be provided instead. There will be a charge for the preparation of the summary or explanation including charge for staff time to develop the summary.

D. The Right to Receive a List of Certain Disclosures of our Health Information That Have Been Made. You have the right to request and receive a list of certain types of disclosures that have been made of your health information. You may not request an accounting for more than a six (6) year period.

HIPAA SCENARIO

A direct care staff informed a consumer about his medication change in the living room in front of other consumers. The staff member was reported to management and the disclosure of PHI was reported to the Privacy Officer. The staff was re-trained on HIPAA Privacy Laws and the agency's policy regarding sharing information.

Requests for this information must be made in writing. The information you may receive will include:

- ☑ The date of the disclosure,
- ☑ The person or organization that received the information and, if known, the address of such entity or person,
- ☑ A brief description of the information disclosed, and
- ☑ A brief reason for the disclosure.

E. The Right to Ask to Correct or Update Your Health Information. If you believe there is an error in your health information or that a piece of important information is missing, you have a right to request that an appropriate change be made. The request must be in writing and state the reason for your request. If approved, the change will be made to your health information and you will be informed of when it was made.

7

WHAT AUTHORIZATION IS REQUIRED FOR USE AND DISCLOSURES OF PHI?

Health care providers may share information with patient authorization, and may share without authorization, for certain purposes, such as:

- During or for the purpose of treatment, for example, axing patient records for a referral
- For payment purposes, including sharing with insurance companies to ensure payment for care
- When employers face workplace injury claims
- When public health researchers need aggregate information for studies
- For health care operations, including contractors and vendors operating on a provider's behalf (subject to security and confidentiality requirements)

HIPAA SCENARIO

A social service agency disclosed PHI while processing Medicaid applications by sending data to computer vendors that were not business partners. New procedures were developed and staff were trained on properly disclosing PHI to only valid business partners.

Written authorization is required for most disclosures of PHI. Your medical provider will provide a waiver or form for you to sign in order for your information to be shared. The authorization or form must be written in specific terms.

Many states have legislated additional protections beyond the general patient rights protections with respect to medical records regarding AIDS/HIV. A legally effective release is a written release of medical information specific to HIV test results, signed by the test subject. A general release is not sufficient. Psychotherapy will also require a separate written authorization as well. Refer to your specific state regulations regarding this issue.

8 WHAT DOES A VALID AUTHORIZATION INCLUDE?

The authorization must specifically identify the PHI to be used or disclosed.

- It must provide the names of the persons or organizations that will receive or use the PHI.
- It must state the purpose for each request.
- It must be signed and dated.
- It must include an expiration date or event.

Individuals have the right to refuse to sign the authorization without negative consequences and may also revoke their authorization at any time.

9 WHAT IS THE "MINIMUM NECESSARY RULE"?

A covered entity must make reasonable efforts to use, disclose and request only the minimum necessary amount of PHI needed to accomplish the intended purpose of the disclosure. In other words, it must only use or disclose the minimum amount of information you necessary to accomplish the task.

10 ARE THERE PENALTIES FOR BREACH AND WHAT ARE THEY?

Yes, there are both civil penalties as well as criminal penalties for noncompliance to the Act. Covered entities may be fined $100 per failure to comply with a Privacy Rule requirement. If the violation was due to reasonable cause and did not involve "willful neglect", and the covered entity corrected the violation within 30 days, then there may not be a penalty imposed by HHS. Criminal penalties can be imposed if a person knowingly obtains or discloses individually identifying health information without proper authorization and can face a fine of $50,000 and up to one year in prison. If the intent is to sell, transfer, or use the PHI for commercial advantage, personal gain, or malicious harm, penalties increase to $250,000 and up to 10 years in prison.

TO OBTAIN A COPY OF THE PRIVACY RULE, AS WELL AS ADDITIONAL MATERIALS, VISIT WWW.HHS.GOV/OCR/HIPAA

HIPAA UPDATES

Effective April 16th, 2024 HHS is applying the confidentiality specifications aspects of CFR Part 2 with HIPAA and HITECH. The changes shall cover the Substance Abuse and Mental Health Services Administration. The new changes include:

Patient Consent: Allows a single consent for all future use and disclosure of information with healthcare. Treatment, payment, and healthcare operations are part of this. Allows the records to be established following the update for all HIPAA Entities and Businesses.

Other Uses and Disclosures: Allows the disclosure of records without patient consent to public health authorities if the records disclosed are de-identified according to the standards in the HIPAA Privacy Rule. Restricts the use of records and testimony in civil, criminal, administrative, and legislative proceedings against patients, unless patient consent is granted or a court order.

Penalties: Replacing criminal penalties currently in Part 2 with civil and criminal enforcement authorities that also apply to HIPAA violations.

Patient Notice: Aligns both Part 2 Patient Notice with HIPAA Notice Patient Notice.

Safe Harbor: Establishing a cap on civil or criminal liability for investigative departments that act with carefulness, to determine if a provider is subject to Part 2 before requesting information during an investigation. The safe harbor mandates that investigative agencies follow specific procedures if they find that they have obtained Part 2 records without obtaining the necessary court order first.

What was modified?

Patient Consent: Prohibits combining patient consent for the use and disclosure of records for civil, criminal, administrative, or legislative proceedings with patient consent for any other use or disclosure. SUD counseling requires a separate patient consent for the use and disclosure of notes. Each disclosure made with patient consent includes a copy of the consent.

SUD Counseling Notes: The clinician voluntarily maintains the notes analyzing the conversation separately from the rest of the patient's SUD treatment and medical record, and that require specific consent from an individual. It cannot be used or disclosed based on a broad TPO consent.

Safe Harbor: Clarifies and strengthens the reasonable steps that investigative departments must follow to be eligible for the safe harbor.

Segregation of Part 2 Data: Adds an express statement that dividing the old and new Part 2 records is not required.

Complaints: Adds a right for all, including patients, to file a complaint directly with the Part 2 program for an alleged violation of Part 2.

Fundraising: Create a new right for patients to opt out of receiving fundraising communications.

PAST MODIFICATIONS

Effective as of March 25, 2013, the following sections in HIPAA have been modified: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and clinical Health Act and the Genetic Information Nondiscrimination Act; Other modifications of the HIPAA Rules. As of September 23, 2013, all covered entities and business associates must comply with the Final Rule.

Breach Notification Rule

A Breach Notification Rule is now defined as "an acquisition, access, use, or disclosure that violates the HIPAA Privacy regulation."

- If there is a low probability that the PHI has been compromised, it is not considered as breach. This regulation does not clearly define "Low probability" so it will be up to the agency's discretion to define this.
- Every situation which involves a potential breach must be analyzed using a risk assessment. "A breach does not include a PHI disclosure where you have a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably be able to retain the PHI."
  - A comprehensive risk assessment should reach a reasonable conclusion based on the following factors:
    - ☑ Whether the PHI of the client was only viewed, or taken into possession.
    - ☑ Classification of the unauthorized individual who used PHI, or who the data was disclosed to.
    - ☑ The amount, type, and details of the PHI involved.
- "Providers have the burden of proof to demonstrate that all notifications were provided to the people whose PHI was breached or that an impermissible use or disclosure did not constitute a breach based on the risk assessment and the documentation of the risk analysis must be maintained."
- From the time the incident becomes known, there is a 60 day window where the person who's PHI has been compromised must be informed.
- The providers are responsible for creating policies and procedures, training employees of the new Breach of Notification rule, and enforce consequences for those who are not in compliance.
- Government analysis will still be responsible for deciding if penalties will be determined, along with the level of fines and fault.

HIPAA Privacy and Security Enforcement

HIPAA outlines the levels of enforcement as follows:

1. If the provider has no knowledge of the violation, or has not exhibited "due diligence," the payment fine ranges from $100 to $50,000 dollars.
2. If the violation results from "reasonable cause," the fine payment ranges from $1,000 to $50,000 dollars. Reasonable cause is defined by HIPAA as an act or omission of the Business Associate or provider knew or could have known that that specific act or omission would be in violation of HIPAA laws.
3. If the violation is a result of "willful neglect"; but if the issue is rectified within 30 days, the fine ranges from $10,000 to $50,000 dollars per violation. If the issue is not rectified within 30 days, the fine payment would be $50,000 dollars or more.
4. $1,500,000 dollars is the maximum amount of money a provider would have to pay per fine per calendar year. Factors that affecting the extent of the fine are as follows:
    a. Any financial or personal harm brought to the person who has had their PHI breached.
    b. Any prior issues with non compliance with HIPAA.
    c. If actions taken to rectify the situation were implemented.
    d. Size of the provider is taken into account, to assess if the fine would negatively impact the providers ability to continue providing services for its clients.

SOURCES

https://www.federalregister.gov/d/2024-02544/p-6

https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/fact-sheet-42-cfr-part-2-final-rule/index.html

https://www.hipaajournal.com/hipaa-updates-hipaa-changes/

https://www.infolawgroup.com/insights/2013/03/articles/hipaa/hipaahitechrules

Privacy Rights Clearinghouse. 2012. https://www.privacyrights.org/

Segalis, B. New HIPAA/HITECH Rules Implementation Roadmap:
Countdown Begins to September 23, 2013 Compliance Deadline. Information Law Group. 2013.
http://www.infolawgroup.com/2013/03/articles/hipaa/hipaahitechrules/

The Substance Abuse & Mental Health Services Administration. 2012.
<http://www.samhsa.gov/>

Clark, L., Esq. HIPAA and Regulatory Compliance (Presentation). September 2011.