Post & Schell P.C.
ATTORNEYS AT LAW

HIPAA And Privacy Update For Post-Acute Care

Mark L. Mattioli
October 4, 2023

Overview

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the use and disclosure of Protected Health Information (PHI) by Covered Entities and their Business Associates

- Certain Entities are deemed Covered Entities, while others may not be

- All members of the workforce who have access to PHI must comply with HIPAA Privacy Policy and Procedures

HIPAA

- **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct (1996)
- Focused on portability of health information, then focused on "administrative simplification"
- It is not an *overall* healthcare privacy rule; only applies to certain entities for certain information in certain settings
- Required the US Department of Health & Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security

HITECH

- **H**ealth **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth (HITECH) **A**ct (2009)
- Made Significant Changes to HIPAA
  - Mandated breach notifications
  - Created tiered civil monetary penalties for non-compliance ranging from $100 to $1,500,000
  - Allowed victims to share in the penalties
  - Expanded enforcement authority to State Attorneys General
  - Imposed direct obligations on Business Associates

HIPAA Omnibus Rule

- Covered entities were required to update various aspects of their HIPAA practices related to privacy and security
  - Expanded individual rights, requiring a new Notice of Privacy Practice to be developed
  - Changes in the expectations of a Business Associate
  - Changes in uses and disclosures related to fundraising and marketing as well as other requirements
  - Result – revise policies and procedures, as well as update forms, and re-educate staff

The Rules Implementing HIPAA

- **Privacy Rule** – individuals' privacy rights and requirements for uses and disclosure of PHI
- **Security Rule** – policies and procedures to protect electronic protected health information
- **Breach Notification Rule** – procedures and timelines for notifications of improper disclosures
- **Enforcement Rule** – penalties for non-compliance

Who Is Subject To HIPAA?

- **Covered Entity**
  - Health plan
  - Health care provider (that transmits any health information in electronic form in connection with a covered transaction – one for which HHS has adopted standards)
  - Clearing houses
- **Not quite a Covered Entity**
  - Business associates

Who Is A Covered Entity?

- **Skilled Nursing –** Yes
- **Assisted Living –** Probably Not
  - Does it provide Health Care and electronically bill?
- **Personal Care Home –** Likely Not
- **CCRC –** Very Likely Not

Business Associates

- A person or entity that:
  - Performs an activity or function on behalf of a covered entity (including claims processing, data analysis, utilization review, and billing) that involves the use or disclosure of PHI; or
  - Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity for a covered entity that involves the use or disclosure of PHI; and
  - Excludes members of the Covered Entity's workforce (employees, volunteers, trainees, etc.)

What Does HIPAA Regulate?

Protected Health Information (PHI)

- PHI refers to a subset of health information that:
  - Is created or received by a health plan, health care provider, employer or health care clearinghouse; and
  - Relates to the payment for health care of an individual, or the past, present or future physical or mental health or condition of an individual, or the provision of health care to an individual; and
  - Identifies the individual or provides a reasonable basis to believe that the information can be used to identify the individual; and
  - Is transmitted by, or maintained in, any electronic media or any other form (including orally or in writing)
- Electronic PHI (ePHI) is PHI that is transmitted by or stored in electronic media

Some Identifiers In Health Information

- Name
- Address (street, city, county or zip code)
- Telephone number
- Fax number
- SSN
- All elements of dates (except for years)
- E-mail address
- Health plan beneficiary number
- Medical record number
- Account number
- Certificate/license number
- Vehicle identifier and serial number
- Device identifier and serial number
- URLs
- Internet Protocol (IP) address numbers
- Biometric Identifiers
- Full face photograph
- Any other unique identifying number or characteristic

Use And Disclosure

- **Use** - The sharing, employment, application, utilization, examination or analysis of individually identifiable health information by any person working for or under the direction of a CE
- **Disclosure** - Any release, transfer, provision of access to or divulging in any other manner of individually identifiable health information to persons not employed by or working under the direction of a CE

When Are Uses/Disclosures Of PHI Authorized?

- **With individual consent** (presumed) - most commonly, for "treatment, payment or health care operations" (TPO)
- **Where individual consent is primarily irrelevant** (national priority purposes) – e.g., mini privacy rules for public health, oversight, litigation, etc.
- **With individual authorization** (consent obtained)
- When "incidental" to a permitted disclosure
- ***Everything else is prohibited***

Use And Disclosure of PHI

- **Mandatory Disclosures:** PHI must be disclosed in two situations:
  - Upon request of the individual who is the subject of the information
  - To HHS in connection with its HIPAA enforcement activities
- **Permitted Disclosures:** PHI may be used and disclosed *without authorization* from an individual:
  - To the individual
  - For TPO purposes
  - Incidental to a permissible disclosure
  - To a Business Associate pursuant to a BAA

Other Permissible Disclosures

- Other uses/disclosures are permitted **without authorization,** subject to certain requirements, if:
  - Required by law
  - About decedent
  - About victims of abuse, neglect or domestic violence
  - Cadaveric organ, eye, or tissue donation
  - For Public health activities
  - Research purposes
  - For Health Oversight activities
  - For law Enforcement Purposes
  - For Judicial or administrative proceedings
  - Specialized government functions
  - To avert a serious threat to health or safety
  - Workers' compensation

Individual Rights

- **Access to Protected Health Information and Requests for Amendment:**
  - Individuals have the right to access and obtain copies of their PHI that the business associate maintains in designated record sets. In addition, individuals may request to have their PHI amended.
  - A CE will provide access to PHI and it will consider requests for amendment that are submitted in writing by individuals with approval from the Covered Entity/Client.
    - Designated Record Set is a group of records maintained by or for the County that includes the payment and claims adjudication records of an individual or other PHI used in whole or in part by or for the Covered Entity to make coverage decisions about an individual.

Individual Rights (cont.)

- **Requests for Alternative Communication Means or Locations:**
  - Individuals may request to receive communications regarding their PHI by alternative means or at alternative locations
  - May grant such requests if they are reasonable and the participant assures that confidentially will not be compromised
- **Requests for Restrictions on Uses and Disclosures of Protected Health Information:**
  - An individual may request restrictions on the use and disclosure of the participant's PHI

Individual Rights (cont.)

- **Accounting:**
  - An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years.
  - Must respond to an accounting request within 60 days. If unable to provide the accounting within 60 days it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60 day period.
  - The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any).
  - If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure. The first accounting in any 12 month period shall be provided free of charge.
  - The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings.

Avoid HIPAA Breaches, Violations And Enforcements

- A Breach is an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI and poses a significant risk of financial, reputational or other harm to the individual
  - Examples: Faxing PHI to the wrong fax number; losing a laptop, flash drive, or CD containing PHI; using a computer infected with a virus or malware; improperly disposing of electronic equipment containing PHI
- If you think there may have been a breach, you must contact the Privacy Officer

Enforcement

- HIPAA contains provisions relating to compliance with investigations by HHS, the imposition of civil monetary penalties for HIPAA violations, and procedures for hearings
- HIPAA also creates criminal penalties for certain violations of patient privacy
- In addition to the harm caused to the Individuals, violations of HIPAA Rules can be costly for Covered Entities and Business Associates

Other Laws That May Apply

- **Pennsylvania Breach Law**
  - Any entity that maintains, stores or manages computerized data that includes personal information must provide notice
- **Personal Information**
  - Includes Health Information
- **Must Encrypt Information**
  - Annually review Policy

NY Breach Law

- Also broadly applicable beyond Covered Entities
- Recent enforcement against law firm that failed to secure health information
  - Fined $200,000

California

- Applies to any entity that collects or retains "Personal Information" of any California resident
  - Medical Information is "Personal Information"
  - Broad definition of Medical Information
- Does not apply to Covered Entities governed by HIPAA
- Applies to larger organizations but can be combined by "Branding"

Notification

- Must be made "as soon as practical" and must utilize a specific form:

[name of institution / logo] date: [insert date]	
Notice of data breach	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web site]

Other States

- Most states now include Medical Information in definition of Personal Information
- Need to Check HIPAA and State Law

FTC Red Flag Rules

- If you do any of these things, you are a Creditor and subject to Rules:
  - defer payment for goods and services or bill customers?
  - grant or arrange credit?
  - participate in the decision to extend, renew, or set the terms of credit?

If So, Do You

- Get or use consumer reports in connection with a credit transaction?
- Give information to credit reporting companies in connection with a credit transaction?
- Advance funds to - or for - someone who must repay them, either with funds or pledged property (excluding incidental expenses in connection with the services you provide to them)?

SNF Breaches

- **Aloha Nursing** - 20,016 patients – Unauthorized computer access
- **Williamsport Home** – Cyber attack
- **Majestic Care** – Unauthorized Access
- **Virtual Care Provider Inc.** – $14M ransomware attack affecting 100 SNFs
- **Catholic Health Care Services** – $650,000 fine of BA
- **Hillcrest Nursing** – $55k fine for lack of access

Hypothetical

- **You inadvertently sent Medical information to another person…..**
  - What is your response?

Hypothetical 2

- **You were hit with a ransomware virus?**
  - Do you need to report it?
  - What do you do?
  - Do you pay the ransom?

Hypothetical 3

- **You caught an Employee looking at records for a relative**
  - Is it a Breach?
  - What do you do?

Hypothetical 4

- **The Police are in the building and want to see medical records to investigate a crime**
  - Do you have to show them the records?

Hypothetical 5

- **You caught an employee downloading information**
  - Can you fire him/her?

Hypothetical 6

- **You received a request for Medical records but don't see any authorization. It is a court case, so do you need to comply?**

Hypothetical 6a

- **Suppose it is a subpoena? Does that make it ok?**

Hypothetical 7

- **A resident eloped, can you provide medical details to the police to help locate him?**

Hypothetical 8

- **The family wants you to change information in the Medical Record. Do you have any obligation to do so?**

QUESTIONS??

Mark L. Mattioli, Esquire
Post & Schell
215-587-1113
mmattioli@postschell.com