Board Education: Health Information Portability & Accountability Act (HIPAA) Training 2024

Presented by :
Rin Coleridge, SFHSS Director of Enterprise Systems and Analytics, HCISSP, CISSP

SAN FRANCISCO
HEALTH SERVICE SYSTEM

HIPAA – What It Is…

Background:

- Comprised of several rules (Privacy, Security, Transaction Code Sets, Breach Notification, Enforcement – HITECH act, Omnibus Rule)
- Protections for privacy of patients and Personally Identifiable Information (PII)
- Covers use and disclosure of Protected Health Information (PHI)
- Sets penalties for breach or data loss when not HIPAA compliant

What HIPAA is:

- Controls what protected health information the Covered Entity can share with employers
- Balance between protecting information and allowing the flow of information
- Individual controls their information (a few exceptions exist)
- Applicable to dependents and to deceased individuals
- Applies to medical, dental, vision, prescription drug, long term care, health and flexible spending accounts.

HIPAA – And Is Not

What HIPAA is not:

- Limitation on health information to the individual – in fact, the covered entity must disclose to the individual who is the subject of the information when requested
- Not applicable to employers, departments/agencies, educational institutions, law enforcement
- Generally, HIPAA does not regulate pharmaceutical companies
- Not applicable to individually identifiable health information held by entities other than covered entities or business associates (BA).
- Not necessarily applicable to wearable health technology / mobile apps
- HIPAA does not apply to long term disability, workers compensation, accident or life insurance.
- HIPAA not applicable to personally identifiable information (PII)

What Information Is Protected?

Identifier

Individually identifiable Health Information, including demographic information (identifies the individual) OR there is a reasonable basis to believe the information can be used to identify the individual.

Health Information

Any information, whether oral or recorded in any form of medium that..

Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse and…

Relates to past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment of the provision of health care to an individual

PHI

Applicability for HSB Commissioners

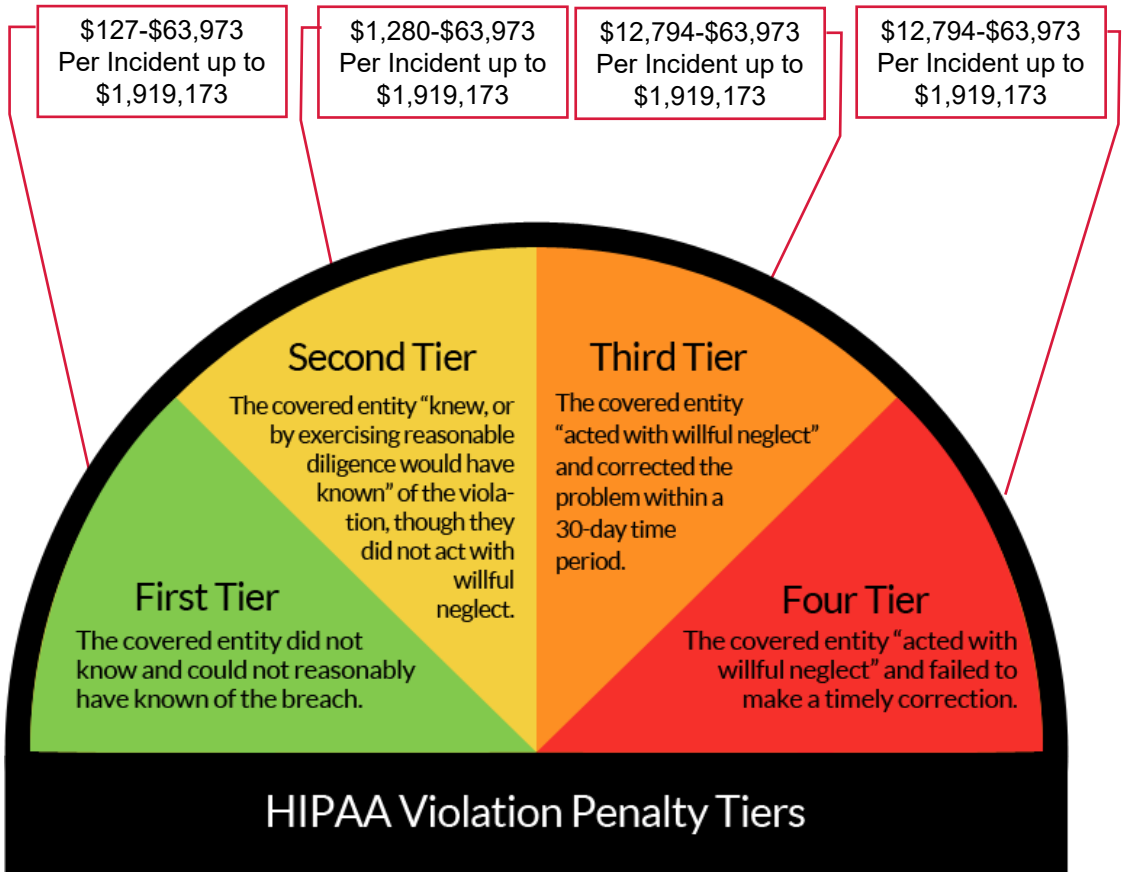
- Protecting each HSS Member's privacy and security is just as important as ensuring the provision of sustainable, quality, health benefits.

- Receive, Consider and Act upon Member 2nd Level Appeals. As part of this process, a significant amount of **Protected Health Information** is shared with the Health Service Board.

- Receive communication directly from SFHSS members outside of the appeals process which also may contain **PHI.**
    - While the member can share any of their information, what you do with that information is governed by HIPAA since SFHSS is a covered entity

- Comply with the HIPAA **Minimum Necessary** requirement and de-identify data using the Safe Harbor method
    - Unless you are a named person with rights to receive the information on behalf of the member (SFHSS has received a HIPAA Authorization from the member for you as an individual), your role as Commissioner does not grant you permission to anything other than the minimum necessary amount of information.
    - Example: Follow up information on what happened for those members who contacted you or participated in the appeal process is not a requirement for resolving the issue.

Penalties



Violations under the HIPAA Privacy Rule don't just include Civil Money Penalties which can result in fines ranging from $127 – $1,919,173 (adjusted for inflation)

Criminal Penalties can result in fines up to $250,000 and up to 10 years in prison. Other consequences of violating HIPAA include lawsuits and restitution, the loss of a medical license or **employee termination**

If more than 500 individuals in a certain geographic area are affected by the breach, the CE must also notify prominent media outlets, HHS and the California State Attorney General's office

Cybersecurity

- Data breaches are a fact of modern life
- In the past, breaches have impacted most of SFHSS' vendors (Medical, Dental, Life Insurance)
- SFHSS has not incurred a breach, but we must remain vigilant
- The human component is the weakest link which is why as Commissioners you have standards to follow

Cybersecurity – Resources / Requirements

- Annual cybersecurity training – coordinated by HSB Secretary
- Comply with **Minimum Necessary** Requirement
- Comply with HSS computer usage standards
  - PHI not kept on the computer – use your network drives
  - Use Multi-factor Authentication (MFA)
  - Never give out your login credentials
- Review guidance found on SFHSS.ORG
  - https://sfhss.org/data-breaches
- HIPAA training is required by HIPAA rules – SFHSS conducts annually
- Use City email account only for HSB business
- Contact SFHSS Privacy Officer if you ever suspect loss or misuse of privacy data or have questions about the types of information to protect and how best to secure it.

2024 – What's New?

- HIPAA Privacy Rule to Support Reproductive Health Care Privacy
  - Announced by Biden-Harris Administration on April 22nd, 2024.
  - Prohibits the use or disclosure of PHI when it is sought to investigate or impose liability on individuals, health care providers, or others who seek, obtain, provide, or facilitate reproductive health care that is lawful under the circumstances in which such health care is provided, or to identify persons for such activities.
  - Requires a regulated health care provider, health plan, clearinghouse, or their business associates, to obtain a signed attestation that certain requests for PHI potentially related to reproductive health care are not for these prohibited purposes.
  - Requires regulated health care providers, health plans, and clearinghouses to modify their Notice of Privacy Practices to support reproductive health care privacy.

APPENDIX

18 Identifiers Which Make Health Information PHI

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, etc.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account Numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

HIPAA Privacy Rule

Covers use and disclosure of PHI. Ultimately with a few exceptions it comes down to the individual to control the information.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.

A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

Required Disclosures. A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.

Permissions Granted by the Privacy Rule

1. SFHSS is allowed to use or disclose PHI for treatment activities, payment activities and healthcare operations (TPO) without the explicit written consent of the individual. NOTE: Not all SFHSS is allowed!
2. To the individual who is the subject of the information
3. Obtain written consent (these must be reviewed by Privacy Officer prior to releasing information)
4. Privacy Officer's Discretion (HHS investigation, ordered by Public Health Officer, safety or health of individual, etc)
5. De-identified data (safe harbor method – suppress 18 identifiers or expert de-identification

HIPAA Security Rule

Deals with electronic Protected Health Information (ePHI).

1. Ensure the confidentiality, integrity, and availability of all e-PHI we create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by our workforce
5. Administrative, technical and physical safeguards