Health Information Portability & Accountability Act (HIPAA)

Rin Coleridge MS, HCISPP | SFHSS HIPAA Privacy & Security Officer

SAN FRANCISCO
HEALTH SERVICE SYSTEM

Introduction

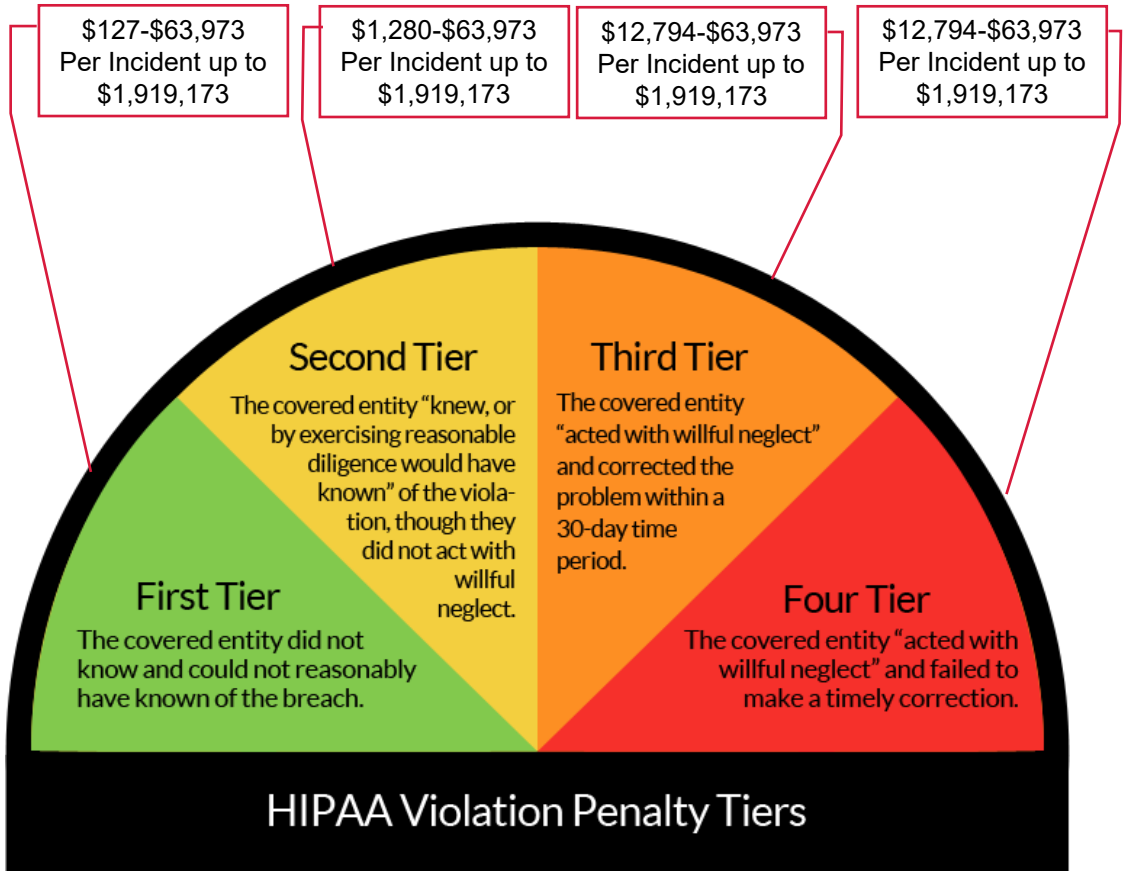
The San Francisco Health Service System (SFHSS) is a Covered Entity and must comply with regulations as outlined in the Health Information Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). As of April 2021, SFHSS has been designated a component of a Hybrid Entity (the City) along with Dept of Public Health, Fire Department, City Attorney, Dept of Technology and Treasurer-Tax Collector.

The compliance requirements extend to Health Service Board Commissioners. This presentation will provide:

- Overview of increases to Civil penalties for not being compliant
- What's new in HIPAA requirements since the January 2022 training
- What new HIPAA Privacy rules are expected for 2023
- Appendix of HIPAA and PHI definitions and role/regulations/practices applicable to Commissioners

HIPAA does not override state law provisions that are at least as protective as HIPAA and therefore SFHSS must ensure compliance with **all** regulations.

HIPAA Criminal and Civil Penalties - Increased Penalties for Civil Violations (effective March 17, 2022)



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

What's New:

- New Interpretation of maximum penalty amounts. Instead of each tier maximum at 1.5M (adj for inflation), the maximum fine was reduced in the first 3 tiers (Tier 1= $25,000, Tier 2 = $100,000, Tier 3 = $250,000)
- December 1, 2022, HHS released guidance regarding the use of Online Tracking Technologies by Covered Entities and Business Associates.

What's Expected:

- There have been no updates since 2013. In 2020 HHS issued proposed rule changes and a Final Rule was expected in 2022. No formal announcement of HIPAA changes has been made.

- There are no planned changes to the HIPAA Security rule.

- Current expectation is new Privacy rules will be implemented in 2023 with enforcement in 2024 aimed at:
  - Easing Certain Administrative Requirements
  - Remove provisions which limited or discouraged care coordination

What's Coming?

- Based on the proposed rule, these are possible changes:
  - Reduce time required to provide access to PHI from 30 days to 15 days
  - Allow patients to review medical record PHI in person and take notes or photos of what they review
  - Allow patients to request a transfer of their PHI to personal health applications
  - Expansion of electronic health record definition to include billing records
  - Modification of the allowed uses of disclosure related to threats to health and safety
  - Allow individuals to direct sharing of PHI maintained in an EHR among covered entities
  - Broaden definition of healthcare operations to cover care coordination and case management
  - Covered Entities will be required to post estimated fees schedules on their websites for PHI access and disclosures
  - HIPAA-covered entities will be required to provide individualized estimates of the fees for providing an individual with a copy of their own PHI

APPENDIX

Role of the Privacy Officer

- Credentials
  - Certified HIPAA Privacy & Security Expert (CHPSE) in 2016
  - HealthCare Information Security and Privacy Practitioner (HCISPP) - 2020

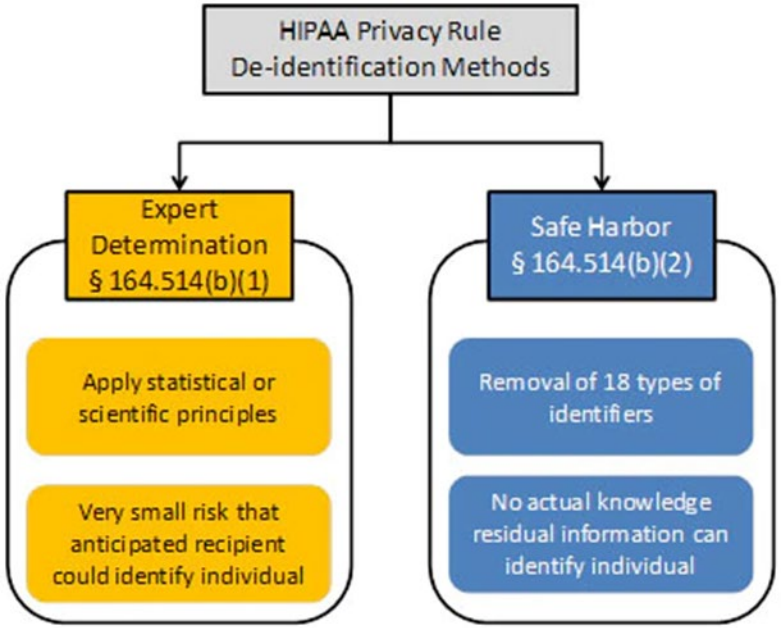
- Develop privacy policies and procedures and implement those policies
- Train members of the covered entity's workforce as to the importance of protecting PHI
- Receive, investigate and respond to requests with regards to PHI
- Log Disclosures
- Regularly monitor and maintain compliance with the covered entity's privacy policies and procedures and the HIPAA Privacy regulations
- Determine classification characteristics of information
- Function as a resource for any questions or concerns. Ask the Privacy Officer prior to releasing information when uncertain.

Role of the HSB Commissioners

- 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
  - 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.
- Compliant with City-wide Cybersecurity training requirements

Permissions Granted by the Privacy Rule

1. HSS 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 HSS 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
5. De-identified data



Practices to Ensure Compliance

- Primary Entity is always accountable for the protection of information
- Minimum Necessary – Limit the amount of personal information collected, used or shared by having a clear purpose for why it is needed.
- Do not discuss any member's details for reasons outside of Treatment, Payment & Operations (TPO)
  - When discussing within the realm of TPO, do so in a secure manner (not during public HSB meetings)
  - Only share with authorized users **who have a need to know it**
- No PHI/PII on Computers. PHI/PII should only be on authorized, secure systems - **City email accounts only**
- If it's hard copy or must be printed, shred when no longer needed
- Phone Communications
- If you don't need it, don't store it.
- Privacy policies and forms: (http://sfhss.org/sfhss-privacy-policy)
- **Complete required training**
- If you ever suspect the loss or misuse of privacy data, or have any questions about the types of information to protect and how best to secure it, contact the Privacy Officer

HIPAA – WHAT, WHY, HOW and WHOM?

- HIPAA governs use, transfer and disclosure of health information
- Health Insurance Portability and Accountability Act (enacted in 1996 / strictly enforced since 2003
- Protects PHI (Protected Health Information)
  - **To Protect the Individual**
    - Protecting personal privacy is to protect the interests and dignity of individuals
  - To Benefit Society through furthering research ethically
    - Protecting patients involved in research from harm and preserving their rights is essential to ethical research
- HIPAA **applies to medical, dental, vision, prescription drug, long term care, health and flexible spending accounts.** HIPAA does not apply to long term disability, workers compensation, accident or life insurance.
- Applies to **Covered Entities**, their Business Associates and Subcontractors

What is Protected Health Information (PHI)?

Under HIPAA, PHI is considered to be any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services.

It is not only past and current health information that is considered PHI under HIPAA Rules, but also future information about medical conditions or physical and mental health related to the provision of care or payment for care. PHI is health information in any form, including physical records, electronic records, or spoken information.

Essentially, all health information is considered PHI when it includes individual identifiers. When we receive it OR create it, we must protect it, **regardless of how it comes to us.**

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. Web 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 & Security Rules

Two Main Elements

- Privacy Rule
- Security Rule

The Privacy rule establishes national standards to protect individuals' medical records and other personal health information.

The Security rule provides layers of protection to protect electronic PHI and ensure its confidentiality, integrity and availability. (**Complete your annual cybersecurity training!)**

- Physical – tangible security controls
- Administrative – management controls
- Technical – technical solutions