

Health Information Portability & Accountability Act (HIPAA)

Rin Coleridge MS | SFHSS HIPAA Privacy & Security Officer

Introduction

The San Francisco Health Service System 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).

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

- Introduction to the HSS Privacy Officer
- Overview of HIPAA and its regulations
- Explanation of penalties for not being compliant
- Review of practices to which all SFHSS employees and commissioners must adhere

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

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

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

You have a role in Privacy Governance!

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

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

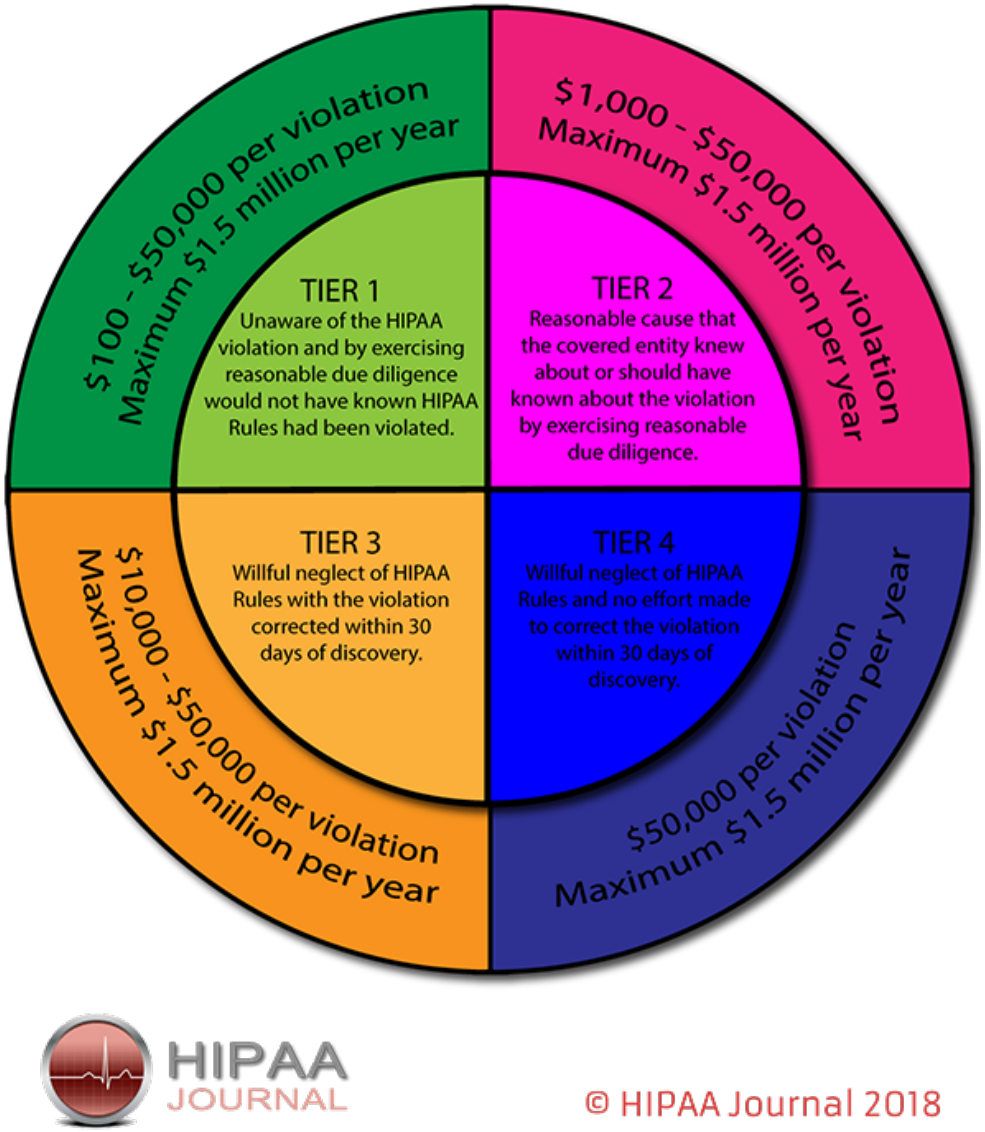
The Privacy rule establishes national standards to protect individuals' medical records and other personal health information.

The Security rule provides layers of protection to protect electronic PHI and ensure its confidentiality, integrity and availability.

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

The Privacy Rule and Security Rule Compared

The Privacy Rule sets the standards for, among other things, who may have access to PHI, while the Security Rule sets the standards for ensuring that only those who should have access to EPHI will actually have access.



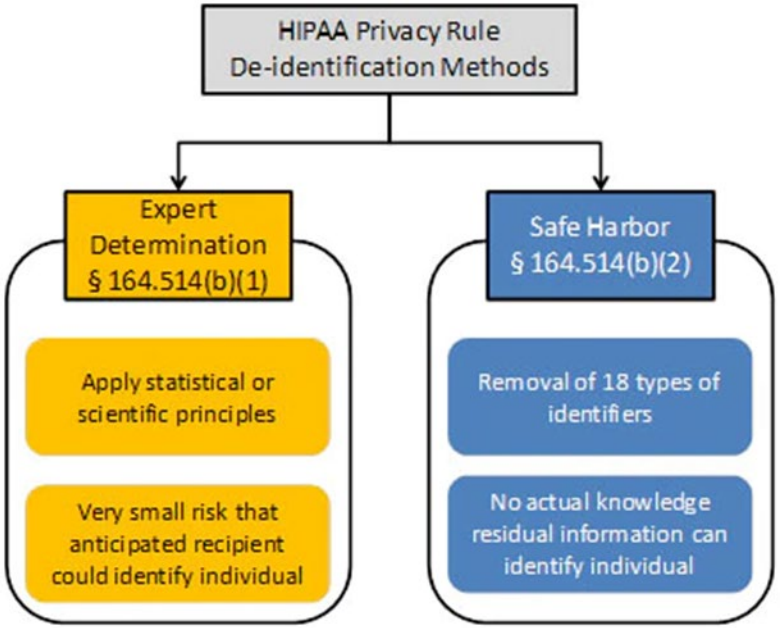
Violations under the HIPAA Privacy Rule don't just include Civil Money Penalties which can result in fines ranging from $100 – $1,500,000

Criminal Penalties can result in fines up to $250,000 and up to 10 years in prison. Other consequences of violating HIPAA include lawsuits, 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

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

- Understand the challenges when it's public officials / info
- Individuals have a right to access their own information
- 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
  - 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. Destroy it in HIPAA compliant manner when it is no longer needed. If you need it, store it in HIPAA compliant manner
- Privacy policies and forms: (http://sfhss.org/sfhss-privacy-policy)
- 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