Board Education:
Health Insurance Portability & Accountability Act (HIPAA)

Presented by
Rin Coleridge, Chief Operating & Experience Officer, SFHSS

August 13, 2026

Agenda

- Introduction
- Definition
- Compliance
- Proposed Changes
- Finalized Changes

Introduction

The Health Insurance Portability and Accountability Act passed in 1996. The rules balance protecting information with allowing information to flow. HIPAA is comprised of multiple rules.

This presentation covers HIPAA requirements, compliance obligations, and recent/proposed regulatory changes. It emphasizes the responsibilities of covered entities and the importance of safeguarding Protected Health Information (PHI).

Definition

HIPAA applies to covered entities:

- Healthcare providers
- Health Plans → (SFHSS / HSB)
- Healthcare Clearinghouse

HIPAA is comprised of several rules:

- Privacy Rule
- Security Rule
- Breach Notification Rule
- HITECH Act
- Omnibus Rule

HIPAA requirements apply to Protected Health Information (PHI):

- Individually identifiable information, including demographic information

AND…

- Health information, whether oral or recorded in any form of medium

Definition continued

HIPAA does not:

Limit health information to the individual.

Apply to entities other than covered entities or their business associates.

Apply to Personally Identifiable Information (PII).

Apply to long term disability*, worker's compensation, accident or life insurance*.

Apply to individually identifiable health information held by entities other than covered entities or Business Associates (BA).

*SFHSS administers LTD, Life and Accident Insurance benefits

Applicability for HSB Commissioners

- Receive, Consider and Act upon Member 2nd Level Appeals.
- Receive communication directly from SFHSS members outside of the appeals process which also may contain **PHI.**
- HSB is bound by HIPAA as part of SFHSS. Once you receive the information, you must now protect it.
- Comply with the HIPAA **Minimum Necessary** requirement and de-identify data using the Safe Harbor method.

Compliance

Requirement	How HSS Complies
Standardized Code Sets	• 834 EDI files
Use and Disclosure of PHI	• Verify member's identity • Obtain authorization prior to release • Release under Treatment, Payment or Operations (TPO)
ePHI administrative, physical and technical safeguards	• Encrypted file transmissions / secure email • Role-based permissions • Intrusion detection • Business Associate Agreements • Secured badge entry • Training
Breach Notifications	• If a breach has occurred, follow notification protocols (to individual, HHS, Media) • Review plan notifications
De-Identified Information	• Apply the safe harbor method to remove 18 identifiers (i.e. Name, SSN) • Minimum Necessary

Civil Penalties

HIPPA Violation Penalty Tiers – Civil Penalties			
Tier	**Violation Standard**	**Penalty Per Violation**	**Per Incident Up To**
First Tier	Covered entity did not know and could not reasonably have known of the violation.	$145-$73,011	$2,190,294
Second Tier	The covered entity "knew, or by exercising reasonable diligence would have known" of the violation, though they did not act with willful neglect.	$1461-$73,011	$2,190,294
Third Tier	The covered entity "acted with willful neglect" and corrected the problem within a 30-day time period.	$14,602-$73,011	$2,190,294
Fourth Tier	The covered entity "acted with willful neglect" and failed to make a timely correction.	$73,011	$2,190,294

Other Repercussions

- Loss of medical license
- Employee termination
- Lawsuits and restitution

Criminal Penalties

HIPPA Violation Penalty Tiers – Criminal Penalties		
Tier	**Violation**	**Maximum Penalty**
First Tier	Knowingly Obtaining or Disclosing	***Up to $50,000 fine and 1 year jail*** for basic unauthorized access or sharing.
Second Tier	False Pretenses	***Up to $100,000 fine and 5 years in jail*** if the information is obtained under false pretenses.
Third Tier	Intent to Sell or Malicious Harm	***Up to $200,000 fine and 10 years in jail*** for commercial advantage, personal gain or malicious intent.

Criminal Penalties

- Fines up to $250,000
- Up to 10 years in prison

Other Repercussions

- Loss of medical license
- Employee termination
- Lawsuits and restitution

Proposed Updates to the Privacy Rule

HSS applicable proposed updates:

- Allow patients to inspect PHI in person and take notes or photographs
- Changes the maximum time to provide access to PHI from 30 days to 15 days
- No longer required to obtain a written acknowledgment from an individual that they have received a Notice of Privacy Practices
- Must post estimated fee schedules on their websites for PHI access and disclosures
- Must provide individualized estimates of the fees for providing an individual with a copy of their own PHI
- Permitted to make certain uses and disclosures of PHI based on their good faith belief that it is in the best interest of the individual
- Must respond to certain records requests from other covered healthcare providers and health plans when individuals direct those entities to do so when they exercise the HIPAA right of access
- The definition of healthcare operations has been broadened to cover care coordination and case management
- Defines when individuals should be provided with ePHI without charge

Proposed Updates to the Security Rule

HIPAA applies to covered entities:

- Technology asset inventory and network map
- Risk analysis
- Contingency planning and security incident response
- Vulnerability scans
- Penetration tests
- Patch management
- Data backups
- Disable unused network ports
- Removal of unnecessary software
- Anti-malware
- Multi-factor authentication
- Annual reviews and tests of security measures
- Annual security rule compliance audits
- Technological safeguards for portable devices
- Require encryption of ePHI at rest and in transit, with limited exceptions

Finalized Changes to the Privacy Rule

Support for Reproductive Health Care Privacy which was announced by the Biden-Harris administration on April 22nd, 2024, was largely struck down.

In June 2025, the U.S. District Court for the Northern District of Texas declared the rule unlawful and vacated it nationwide.

- ~~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.

Summary

Key topics covered in this training:

- HIPAA fundamentals
- What HIPAA does not cover
- Applicability to HSB Commissioners
- Compliance practices
- Penalties for violations
- Proposed and implemented updates to the Privacy and Security Rules
- Key reminders:
  - 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
    - Never give out your login credentials
  - Review guidance https://sfhss.org/data-breaches
  - 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.

Appendix

What Information is Protected?

Identifier + **Health Information** = **Protected Health Information**

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.

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.

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