

Superstition Fire & Medical District



HIPAA Awareness and the
Protection of Patient Privacy

SFMD HIPAA Training

- The Health Insurance Portability and Accountability Act (HIPAA) requires compliance in protecting the confidentiality and integrity of health information and patients' rights to privacy.
- To comply with the HIPAA standards, all members of the Superstition Fire & Medical District and anyone who may be accompanying members of the Fire District must complete Health Insurance Portability and Accountability (HIPAA) training.



- This is a self-study program explaining HIPAA.
- This self-study program is a mandatory training requirement for any person who is interested in being able to ride along with SFMD.
- Each person is responsible for understanding HIPAA and following AJFD guidelines/policies pertaining to patient privacy.

SFMD HIPAA Training

Purpose

- To ensure that all members of Superstition Fire & Medical District Staff---including all employees, volunteers, students, and trainees (collectively referred to as “members”) who have access to patient information understand the organization’s concern for the respect of patient privacy and are trained in the District’s policies and procedures regarding HIPAA regulations and Protected Health Information (PHI).

Purpose

- Provide an overview of federal and state laws concerning patient privacy including the Privacy Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Describe protected health information (PHI)
- List the patient rights under the HIPAA Privacy Rule
- Understand the importance and benefits of privacy compliance
- Explain the consequences of failure to follow established privacy policies

Objectives

- HIPAA = Health Insurance Portability and Accountability Act of 1996



What is HIPAA?

Who is Affected by HIPAA?

- “Covered Entities”
 - Health plans,
 - Health care clearinghouses, or
 - Healthcare providers
 - A provider of medical or health services and any other person or organization that furnishes, bills, or is paid for healthcare in the normal course of business



- Give patients more control over use of data
- Set boundaries on uses and disclosures of data
- Establish safeguards to protect data
- Establish accountability for privacy breaches
- Balance privacy with social responsibility
- To safeguard and protect the confidentiality and integrity of a person's Protected Health Information

What is HIPAA designed to do?

- Protected Health Information (PHI)
- PHI is information that:
 - Relates to an individual's physical or mental health, treatment, or payment
 - Information that is created or received by a health care provider, health plan, employer, life insurer, school or university, or health care clearinghouse
 - Information relating to the past, present or future physical or mental health or condition of an individual

HIPAA and PHI

- PHI information (*Cont.*):
 - Identifies the individual or gives a reasonable basis to believe that the individual can be identified
 - Is transmitted or maintained in any format
 - Oral statements
 - Electronic information
 - Written material
 - Photographic material

HIPAA and PHI

What Information Is Covered Under HIPAA?

- Examples of individually identifiable health information:
 - Name
 - Address
 - Employer
 - Relative's names
 - Dates relating to patient
 - Phone & fax numbers
 - Finger or voice print
 - Photograph
 - Medical treatment given
 - Health plan beneficiary number
 - E-mail address/URL
 - Social security number
 - Medical record number
 - Employee or account number
 - Vehicle or device number
 - License numbers
 - Any unique identifier or code

What Information Can be Shared Under HIPAA?

- What hospital patient was transported to
- Method of transportation (*Helicopter, Ambulance*)
- General location of incident
- General condition of patient (*Minor Inj., Stable, Critical*)

- Patients are given broad new rights under the Privacy Rule including:
 1. Notice of privacy practices/policies
 2. Consent (optional)
 3. Authorization
 4. Access
 5. Amendment
 6. Accounting
 7. Recourse

“HIPAA Rights”

- We may use and disclose the patient's PHI for three purposes without any written consent, authorization, or other approvals from the patient. These purposes are:
 - Treatment
 - Payment
 - Healthcare operations ("TPO")
- Must be written in plain language
- Patient must be informed of right to request restrictions
- References privacy notice
- May be combined with other consents (but not privacy notice)
- No expiration date
- Signed & dated
- Revocable by the patient at any time

"HIPAA Rights" - Consent

- If we wish to use or disclose the patient's PHI for any purpose other than treatment, payment, or healthcare operations, a signed authorization form must be obtained from the patient or his/her authorized representative.

"HIPAA Rights" - Authorization

"HIPAA Rights" - Authorization

- Authorization - Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required
 - Required by law
 - Public health activities (injury/disease control/prevention)
 - Victims of abuse, neglect, or domestic violence
 - Health oversight activities (DHS, regional EMS council)
 - Judicial and administrative proceedings
 - Decedents
 - Cadaveric donation of organs, eyes, or tissues
 - Research purposes
 - To avert a serious threat to health or safety

- If the patient is incapacitated or in cases of an emergency, we may, in the exercise of professional judgment, determine whether disclosure of PHI is in the patient's best interests.
 - For example, this provision of the Privacy Rule allows us to inform relatives or others involved in a patient's care that a patient has suffered a heart attack and to provide updates on the patient's progress and prognosis.
- In these situations, disclose only the PHI that is directly relevant to the person's involvement with the patient's healthcare.

Special Situations

Special Situations

- Patients with HIV
 - Criminal offense to reveal information
 - No patient may be tested for HIV or AIDS without their consent
 - No information regarding the results of these tests may be provided to anyone other than the patient

Special Situations

- Psychiatric Patients & Substance Abuse
 - Violation of federal law to reveal or confirm the identity of a patient in any psychiatric or drug / alcohol program.



Special Situations

**Why should I worry about
HIPAA?**

Failure to Comply - "Sanctions"

- Reputation of organization
- Employee disciplinary action
 - May include termination
- Civil fines
- Criminal fines and imprisonment



- Civil penalties
 - Violators that unintentionally disclose information will be subject to penalties of \$100 per violation, up to \$25,000 per person, per year for each requirement or prohibition violated.



HIPAA Penalties / Sanctions

HIPAA Penalties / Sanctions

- Federal criminal penalties
 - Up to \$50,000 and one year in prison for obtaining or disclosing protected health information
 - Up to \$100,000 and up to five years in prison for obtaining protected health information under "false pretenses"
 - Up to \$250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain, or malicious harm



Complaints of Violations

- Any patient may complain to the organization's Privacy Officer or to the U.S. Department of Health and Human Services
 - Organizations must respond promptly and take appropriate action as needed



SFMD and HIPAA Compliance

SFMD Policy Statement

- Given the nature of our work, it is imperative that we maintain the confidentiality of patient information that we receive in the course of our work.
- SFMD prohibits the release of any patient information to anyone outside the organization unless required for purposes of treatment, payment, or healthcare operations.
- Discussions of Protected Health Information (PHI) within the organization should be limited.



- Acceptable uses of PHI within the District include, but are not limited to:
 - Exchange of patient information needed for the treatment of the patient
 - Billing and other essential healthcare operations
 - Peer review
 - Internal audits
 - Quality management activities

SFMD Policy Statement

- Superstition Fire & Medical District members must comply with all confidentiality policies and procedures set in place by the District during their employment or association with SFMD.
 - 'Members' = all employees, volunteers, students, trainees, and ***Ride-Along Partners***

SFMD Policy Statement

- If a member knowingly or inadvertently breaches patient confidentiality policies and procedures at any time, the member must immediately notify the SFMD Privacy Officer or their immediate supervisor.

SFMD Policy Statement

Policy

- All new members will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time upon association with the organization.

SFMD Policy on Privacy Training

Procedure

- Training will be conducted in the following manner:
 - Computer-based PowerPoint presentation with required post-test to be submitted to the Privacy Officer upon completion of training.

SFMD Policy on Privacy Training

- When PHI is accessed, disclosed, and used, the individuals involved will make every effort, except in patient care situations, to only access, disclose, and use PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose.

SFMD Member Access to PHI

- Fire District members must be sensitive about the importance of maintaining the confidence and security of all material we create or use that contains patient care information.
- Co-workers and other members should not have access to information that is not necessary for the member to complete his or her job.

SFMD Member Access to PHI

Confidentiality

- Avoid disclosures to anyone who is not involved in patient care.
- Pay attention to who is within earshot when a member makes a verbal statement about a patient's health information, and follow some of these common sense procedures for avoiding accidental or inadvertent disclosures ...

Confidentiality

- Facilities and Waiting Areas:

- If patients are in waiting areas to discuss the service provided to them or to have billing questions answered, make sure there are no other persons in the waiting area, or if so, bring the patient into a private area before engaging in discussion.

Confidentiality – Verbal Security

Confidentiality – Verbal Security

- Public Areas:
 - Be sensitive to that fact that members of the public and other agencies may be present in easily accessible areas.
 - Conversations about patients and their healthcare should not take place in areas where those without a need to know are present.



- Other Areas:

- Members should only discuss patient care information with those who are involved in the care of the patient, regardless of their physical location.
- On emergency scenes you may be approached by other by-standers and asked questions regarding the patient that could violate their PHI. ALWAYS let these people know you are just an observer and refer them to SFMD personnel for further information.

Confidentiality – Verbal Security

HIPAA Training....

... In Conclusion

- Remember, you have an obligation to maintain any confidential PHI you may encounter during your Ride-Along experience with the Superstition Fire & Medical District

“What you hear here,
What you see here,
Let it stay here,
When you leave here.”



- Please complete the post-test.
- Please read and sign the “Acknowledgement of HIPAA Obligations” form.
- **Return the completed post-test and signed form to the Superstition Fire & Medical District Training Center.**
 - Receipt of these documents will serve as verification of the federal HIPAA training requirement.

HIPAA Training Complete...

HIPAA Training Complete

...Thank you!

...Thank you!