

HIPAA Training for Volunteers

SHFC

2016

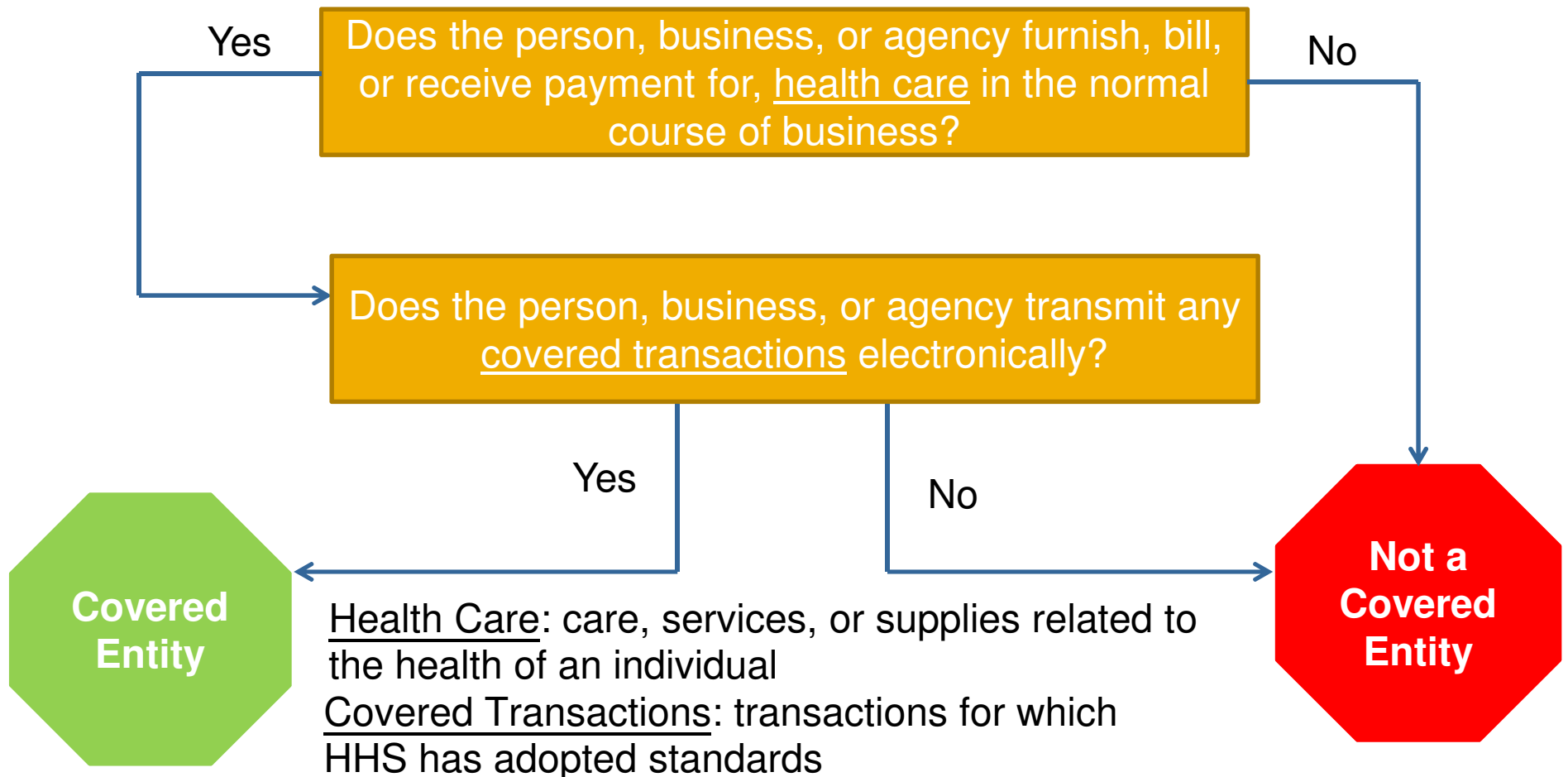



What is HIPAA?

- **HIPAA** stands for the Health Insurance Portability and Accountability Act
- HIPAA is implemented through four regulations:
 - Privacy Rule
 - Security Rule
 - Breach Notification Rule
 - Enforcement Rule
- The regulations have evolved over the past decade, generally becoming more restrictive over time.

Who Must Comply With HIPAA?

Is a person, business, or agency a Covered Entity?





Privacy Rule

Introduction

Protected Health Information (PHI)

- The privacy rule protects information that is individually identifiable to a patient.
- Provides for individual rights with respect to PHI
- Imposes administrative requirements including requiring designation of a privacy officer, conducting HIPAA training, and documenting and implementing policies and procedures

Patient Identifiers

- Names
- Address (street, city, county or zip code)
- Telephone numbers
- Social Security numbers
- All elements of dates (except for years)
- E-mail address
- Full face photographs
- Any other unique identifying number or characteristic

Expectations

- All face to face conversation with an individual that addresses PHI needs to happen in a private area.
- The hallway outside of the exam rooms and the area around the pharmacist and coordinator need to be clear of people waiting.
- Medical records need to be protected in the public clinic areas by being placed face down - other people should never have access to someone's medical record or our nightly logs.
- All medical records will be stored in a locked area.
- All garbage with PHI will be shredded.
- PHI should not be disclosed over the phone unless talking to the individual or with permission to leave a message documented in the medical record.

Uses and Disclosures

When can SHFC use & disclose PHI?

SHFC can use & disclose PHI for the purpose of treatment and health care operations

TREATMENT

the provision, coordination, or management of health care by one or more health care providers , including consultation between providers and patient referrals

HEALTH CARE OPERATIONS

are administrative, financial, legal and quality improvement activities

Other Permitted Uses & Disclosures

Other Uses and Disclosures Include:

- To prevent a serious and imminent threat to health and safety of the patient, another person, or the public
- For required public health disease surveillance and monitoring
- To contact and remind patients of an upcoming healthcare appointment or referral information
- In the course of legal proceedings, if required to do so by a court or a judge

Authorization to Use or Disclose PHI

In general, an individual must authorize uses and disclosures of their PHI

- The Coordinator has release forms for patient to sign and authorize disclosure of PHI as indicated.
- Contact the SHFC Privacy Officer (Jennifer Hyatt) if you are unsure of the process.

Minimum Necessary Standard

- Uses or disclosures of PHI, even where authorized, must be limited to the “minimum necessary” to accomplish the intended purpose
 - Exceptions: Disclosures to health care providers for treatment purposes, disclosures to the individual, or disclosures made pursuant to an authorization
- Uses
 - If you do not need to know confidential or sensitive information to do your job, you should not have access to it
 - You should not review files of patients you are not caring for
- Disclosures
 - Only share the least PHI that meets the need and level of authorization of recipient
 - Generally, it is not permissible to share an entire medical record without patient authorization
 - You may rely on requests from public health officials, or other covered entities

Individual Rights

Patients have certain rights, including, but not limited to

- Right to access PHI
- Right to amend PHI
- Right to request restrictions on the use and disclosure of PHI
- Right to have reasonable requests for confidential communications of PHI accommodated
- Right to notice of a breach of PHI
- Right to file a complaint with Office for Civil Rights
- Right to a written Notice of Privacy Practices

Notice of Privacy Practices

- Each patient must receive a written Notice of Privacy Practices (NPP).
- The NPP tells patients about SHFC privacy policies and practices and ways their information will be used.
- The NPP also details individual rights, including the right to obtain copies of PHI and/or request amendments.
- SHFC must make a good faith effort to obtain the patient's written acknowledgment that they received a copy of the NPP.
- If patient refuses to sign the NPP, please document - initial & date Notice along with brief reason for refusal.



Security Rule

Introduction

- The Security Rule protects the subset of PHI that a Covered Entity creates, receives, maintains, or transmits in *electronic form* (ePHI).
- The Security Rule generally requires a Covered Entity and its business associates put into place a number of safeguards to protect ePHI in their possession.
- The Security Rule Safeguards are divided into three categories:
 - Administrative Safeguards (such as policies and procedures)
 - Physical Safeguards (such as locks, doors, walls)
 - Technical Safeguards (such as automatic log-off, passwords, encryption and decryption, & user verification)

Recent Focus on the Security Rule

The Security Rule has traditionally not been a major compliance focus for Covered Entities, but this has changed due to:

- A industry-wide shift to electronic transactions and electronic medical records.
- Increasing use of removable media and remote access.
- Increasing number of instances of highly publicized, improper disclosures of ePHI.

Physical Safeguards

- **Facility and Access Control**
 - Limit physical access to ePHI and ensure any access is authorized.
- **Workstation and Device Use**
 - Facilitate proper use of and access to workstations and electronic media



Breach Notification Rule

Introduction

∇ A “Breach” is

An impermissible use or disclosure of PHI that compromises the security or privacy of the PHI and poses a significant risk of financial, reputational, or other harm to the individual.

∇ If you think there may have been a breach, please contact Jennifer Hyatt/ SHFC Privacy Officer by either:

Calling the SHFC phone at 406-261-7541 or
Filling out an encounter form and placing it in her mailbox in the SHFC office.



Enforcement Rule

Enforcement

- HIPAA also contains provisions relating to compliance with investigations by HHS, the imposition of civil monetary penalties for HIPAA violations, and procedures for hearings.
- In addition, HIPAA creates criminal penalties for certain violations of patient privacy.

*Ignorance of the HIPAA law
is NO DEFENSE!*

In Conclusion

All SHFC volunteers will operate under the "minimum necessary standard" which expects you to use only the information you need to perform your role at the clinic. This includes face to face interaction as well as information contained in the patient's medical record.

All volunteers have a duty and responsibility to protect patient information and privacy.

As a volunteer of SHFC you are expected to understand the HIPAA regulations. You will be able to access detailed information on our website if at any time you need further information or clarification.