HIPAA Training for Providers

[Organization]

[Date]

What is HIPAA?

- **HIPAA** stands for the Health Insurance Portability and Accountability Act of 1996, which became law on August 21, 1996.
- 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.

Overview of HIPAA

HIPAA **(Health Insurance Portability and Accountability Act of 1996)**	• Became law on August 21, 1996. • Federal regulations enacted under HIPAA in 2002 and 2003, known as the Privacy Rule and the Security Rule, created national requirements that protect medical records and other personal health information, known as protected health information or "PHI." • The Privacy and Security Rules apply to "Covered Entities" and "Business Associates." • The HIPAA Enforcement Rule was later passed in February 2006 and established final penalties for any and all HIPAA violations.
HITECH **(Health Information Technology for Economic and Clinical Health Act)**	• Enacted on February 17, 2009 and made significant changes to HIPAA. • The HITECH Act strengthened HIPAA enforcement by (among other things): 1. Requiring Covered Entities and their Business Associates to notify affected individuals, the Secretary of HHS and, in certain cases, the media, of breaches of unsecured protected health information; 2. Creating a new tiered civil monetary penalty structure with penalty amounts ranging from $100 to $1,500,000 depending on an entity's perceived culpability for the HIPAA violation; and 3. Expanding HIPAA enforcement ability to state attorneys general and allowing for sharing of penalties with individuals harmed by a HIPAA violation, and 4. Making the Security Rule and portions of the Privacy Rule regulations directly applicable to Business Associates.
HIPAA Omnibus Rule	• Released on January 17, 2013 and effective on March 26, 2013. • The Omnibus Rule modified the HIPAA Privacy, Security, and Enforcement Rules to implement statutory requirements of the HITECH Act.

Who must comply with HIPAA?

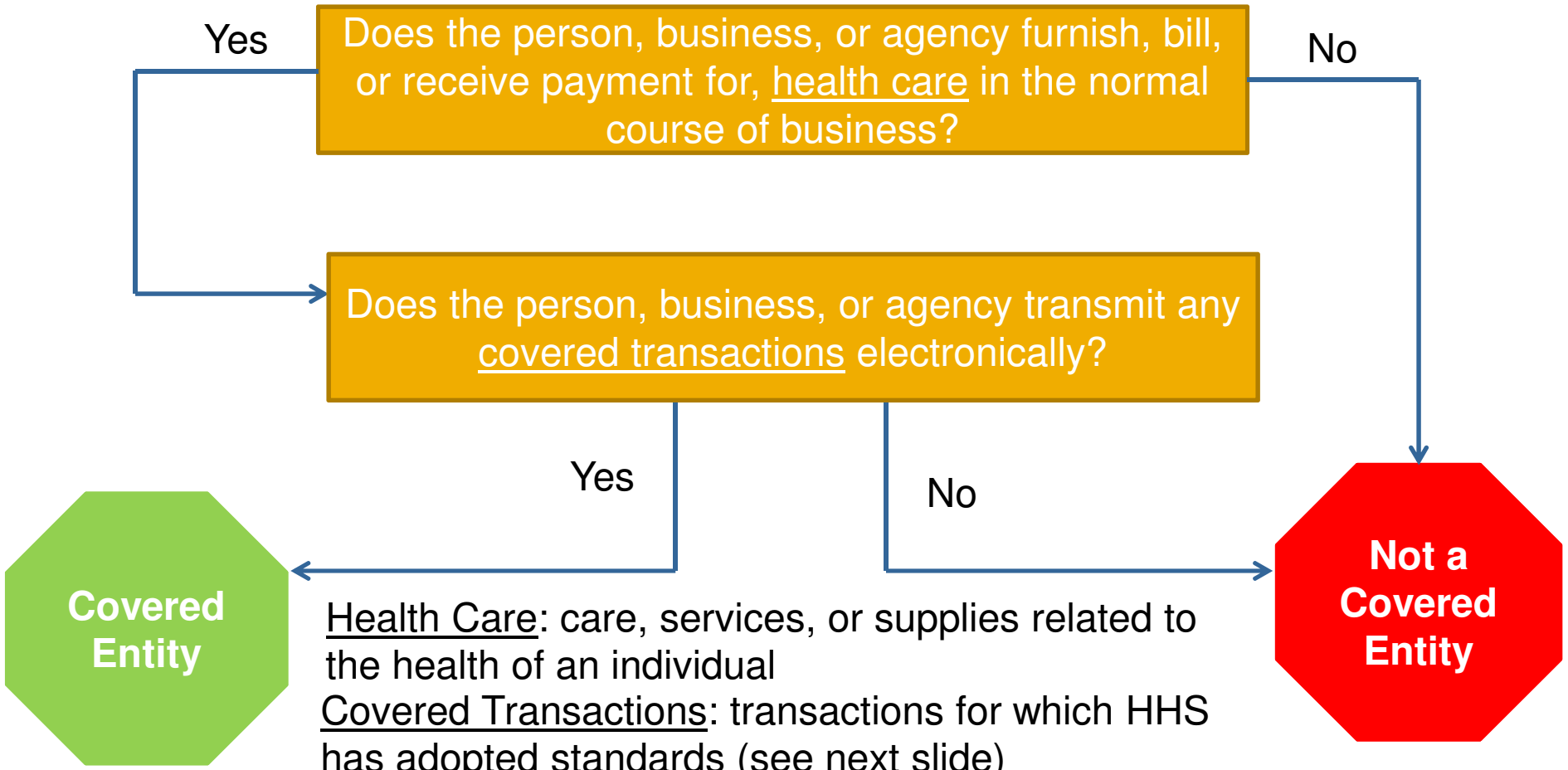
The HIPAA Rules apply to "Covered Entities" and "Business Associates."

Covered Entities include certain health care providers, health plans, and health care clearinghouses, such as:

- Hospitals
- Physician practices
- Home care agencies
- Ambulatory surgery centers
- Health systems
- Imaging centers
- Health insurance companies
- Group health plans that are employee welfare benefit plans, also known as "self-insured" plans

Who Must Comply With HIPAA?

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



Health Care: care, services, or supplies related to the health of an individual

Covered Transactions: transactions for which HHS has adopted standards (see next slide)

Who Must Comply With HIPAA?

Examples of HIPAA Covered Transactions (if submitted electronically)

Health Care Claims	Health Plan Transaction
• A request to obtain payment, and necessary accompanying information, from a health care provider to a health plan. • The transmission of encounter information for the purposes of reporting health care.	• An inquiry from a health care provider to a health plan, to obtain information about eligibility, coverage, or benefits. • Referral requests or requests to obtain an authorization for health care.

Who must comply with HIPAA?

Business Associates include any person or entity that:

- Performs an activity or function on behalf of a covered entity (including claims processing, data analysis, utilization review, and billing) that involves the use or disclosure of PHI, or
- Provides legal, actuarial, accounting, management, administrative, accreditation or financial services for a covered entity that involves the use or disclosure of PHI.

Examples of Business Associates:

- A law firm providing malpractice claim advice to a hospital (if representation requires disclosure of PHI).
- A provider of electronic health record software that provides service support (if support involves viewing of PHI).

What information is protected by HIPAA?

HIPAA applies to Covered Entities' handling of Protected Health Information ("PHI")

PHI is a subset of health information that:

- Is created or received by a health plan, **health care provider**, employer or health care clearinghouse; and
- Relates to the **payment** for health care of an individual, or the past, present or future **physical or mental health or condition** of an individual, or the **provision of health care** to an individual; and
- **Identifies the individual** or provides a reasonable basis to believe that the information can be used to identify the individual; and
- Is transmitted by, or maintained in, any electronic media or any other form (including orally or in writing).

Patient Identifiers

- Names
- Address (street, city, county or zip code)
- Telephone numbers
- Fax numbers
- Social Security numbers
- All elements of dates (except for years)
- E-mail address
- Health plan beneficiary numbers
- Medical record numbers
- Account numbers

Patient Identifiers (*continued*)

- Health plan beneficiary numbers
- Medical record numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Uniform Resource Locator (URLs)
- Internet Protocol (IP) address numbers
- Biometric Identifiers
- Full face photographs
- Any other unique identifying number or characteristic

Privacy Rule

Introduction

- Requires that PHI be used or disclosed *only* with patient authorization or as permitted by the rule
- Limits use and disclosure to the minimum amount of PHI necessary to achieve the purpose of the use or disclosure
- 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

Uses and Disclosures

Permitted uses and disclosures:

- For "treatment, payment or health care operations."
- After the individual is provided an opportunity to agree or object to the use/disclosure.
  - For example, limited disclosures to family members and other persons involved in the individual's care, if the individual is able to consent to the disclosure
- For a specific permitted purpose and meets the requirements related to that purpose.
  - For example, disclosures to a public health authority about a communicable disease
- "Incidental" to a permitted disclosure.
  - For example, when a patient hears another patient's name called out in the waiting room

"TPO" Uses & Disclosures

Most routine uses and disclosures of PHI by Covered Entities are for "Treatment," "Payment," or "Health Care Operations" purposes.

"Treatment" consists of:

- The provision of health care services.
- Coordination and/or management of health care and related services between one or more health care providers, or a health care provider and a third party.
- Consultation between health care providers relating to a patient.
- The referral of a patient for health care from one health care provider to another.

“TPO” Uses & Disclosures

“Payment” consists of:

- Determining eligibility or coverage under a plan and adjudicating claims
- Risk adjustments
- Billing and collection activities
- Reviewing health care services for medical necessity, coverage, justification of charges, and the like
- Utilization review activities
- Disclosures to consumer reporting agencies (limited to specific identifying information about the individual, the individual’s payment history, and identifying information about the covered entity)

"TPO" Uses & Disclosures

"Health Care Operations" may include:

- Case management and care coordination.
- Quality assessment and quality improvement
- Business planning and administration, such as conducting cost-management analyses.
- Due diligence in connection with the sale or transfer of assets to a successor in interest (if such successor is, or following the sale will become, a covered entity).

Health Care Operations must relate to the Covered Entity's covered Functions.

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
- For fundraising purposes, if fundraising materials provide an opportunity to opt out of future communications
- 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 other than for TPO

- The authorization permits use and disclosure by a Covered Entity or by a third party.
- The authorization must include certain phrases that are described in the Privacy Rule regulations.
- [If you need to use or disclosure PHI outside of TPO, please consult [Company's] HIPAA Authorization Policy and Form.]

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, other covered entities, researchers with IRB approval, our Business Associates, so long as the Business Associate states the request complies with the minimum necessary standard
  - [[Company] has policies in place regarding routine disclosures such as [insert]]
- [If you have a question about what constitutes the "minimum necessary," please contact [Company's Privacy Officer]

Individual Rights

- Right to access PHI
- Right to amend PHI
- Right to receive an accounting of disclosures of PHI
- Right to request restrictions on the use and disclosure of PHI
- Right to pay out-of-pocket for treatment without reporting to a health plan
- 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

Patient Access to ePHI

- Covered Entity must provide individuals with access to their PHI held by Covered Entity upon request.
- Covered Entity may charge the individual a reasonable, cost-based fee for a copy of the requested PHI.
- Covered Entity must approve or deny, or provide access to PHI, within 30 days of the request.
- [If a patient requests access to their PHI, please consult [Company's] Patient Requests for PHI Policy.]

Accounting of Disclosures

- Tracking of Disclosures
  - Covered Entity must provide the date of disclosure, the name of the recipient, a description of the PHI disclosed, and the purpose of the disclosure for all disclosures except those related to TPO, incidental disclosures, and pursuant to an authorization.
- Covered Entity must provide a patient with an accounting of disclosures of their PHI without charge once every 12 months.
- Covered Entity may impose a reasonable, cost-based fee for each subsequent request during the 12-month period
- [If a patient requests an accounting of disclosures of his/her PHI, please consult [Company's] Accounting of Disclosures policy]

Notice of Privacy Practices

- Each patient must receive a written Notice of Privacy Practices (NPP).
- The NPP tells patients about a Covered Entity's 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.
- A Covered Entity must make a good faith effort to obtain the patient's written acknowledgement that they received a copy of the NPP.
- If a Covered Entity maintains a website, the NPP must be prominently posted on the Covered Entity's website.

Administrative Requirements

- Privacy Official – responsibility for privacy must be assigned to a “high ranking” individual within a Covered Entity.
- Business Associates – written contracts must be in place in order to safeguard PHI.
  - [Before disclosing PHI to a contractor of [Company], consult the Privacy Officer to ensure that a “Business Associate Agreement” is in place.]
- Written Policies and Procedures – required to protect patient PHI.
- Workforce Training – must be conducted in order to ensure compliance.

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, identification badges); and
  - Technical Safeguards (such as automatic log-off, passwords, encryption and decryption, user verification, and audit controls).

Recent Focus on the Security Rule

The Security Rule has traditionally not been a major compliance focus for Covered Entities or Business Associates, 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.

Recent Focus on the Security Rule

Examples of recent, high-profile Security Rule violations:

- Hacking of University of Washington Medical System computer system (over 4,000 records accessed).
- Kaiser-Permanente mistakenly e-mailed highly sensitive personal health information to wrong members.
- The University of Montana posted psychological records of at least 62 children and teenagers on a public website.
- Eli Lilly accidentally e-mailed the e-mail addresses of all Prozac users who had signed up for e-mail reminders to the entire list.

Administrative Safeguards

- Security Management Process
  - Risk Analysis: Assess vulnerabilities of current technologies, potential threats, and extent of harm in order to assign levels of risk, and
  - Risk Management: Implement strategies and new technologies in order to reduce risk identified in risk analysis to acceptable levels.
- Security Personnel
  - Designate a Security Officer,
  - Institute information access management,
  - Provide workforce training,
  - Develop security incident procedures and a contingency plan, and
  - Perform routine evaluations of security policies/procedures.

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,
  - Transfer, remove, dispose of and reuse media appropriately, and
  - Consider encrypting all devices that access ePHI.

Technical Safeguards

- Access control – assign user rights/privileges to limit access ePHI, based on job function, consisting of:
  - Unique user identification,
  - Emergency access procedure,
  - Automatic logoff, and
  - Encryption and decryption of data in transit.
- Audit controls – implement a system for recording and examining system activity.
- Integrity – protect ePHI from improper alteration or destruction.
- Authentication – verify that a person or entity seeking access to ePHI is the person claimed.
- Transmission Security – implement measures that protect ePHI while it is being transmitted, through the use of integrity controls and encryption.

Breach Notification Rule

Introduction

- A "Breach" is

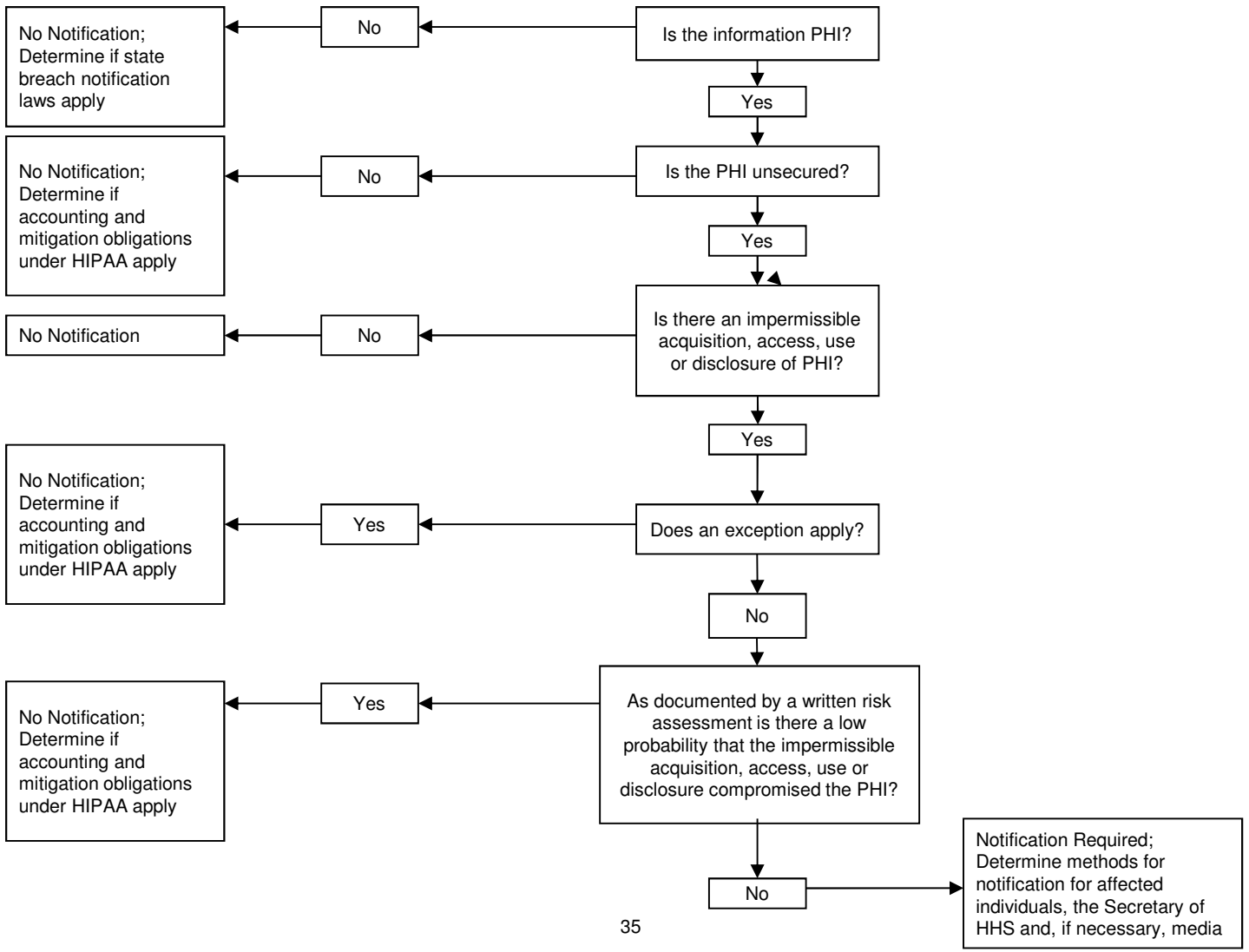
  An impermissible use or disclosure of PHI that compromises the security or privacy of the PHI and poses a significant risk of financial, reputational or other harm to the individual.

- If you think there might be a breach, please contact [Company's Privacy/Security Official].

Examples of Possible Breaches

- Faxing patient information to the wrong fax number.
- Losing a laptop, flash drive, or CD containing patient information.
- Having improper website security that exposes an internal part of the website containing PHI to the public.
- Using a computer infected with a virus or malware.
- Improperly disposing electronic equipment containing PHI.

Breach Analysis Flow Chart



Enforcement Rule

Introduction

- 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.

What Makes a Violation Criminal

- The HIPAA criminal enforcement provision can be violated when a person knowingly:
  - Uses or causes to be used a unique health identifier;
  - Obtains individually identifiable health information relating to an individual; or
  - Discloses individually identifiable health information to another person.

Criminal Penalties for HIPAA Violations under 42 U.S.C. § 1320d-6	
Any Violation	• Applied for any offense. • $50,000 fine, one year imprisonment, or both.
False Pretenses	• Applied if the offense is committed under false pretenses. • $100,000 fine, 5 years imprisonment, or both.
Advantage, Gain, or Harm	• Applied if the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. • $500,000 fine, 10 years imprisonment, or both.

Common Privacy Complaints

- Impermissibly using or disclosing an individual's health information.
  - Example: A hospital leaves a detailed message at the wrong phone number.
- Failing to implement adequate safeguards to protect PHI.
  - Example: A pharmacy log book is left in plain view of customers.
- Refusing or failing to provide an individual with access to their PHI.
  - Example: A physician practice denies patients who want to change practices copies of their records.
- Disclosing more data than is minimally necessary to satisfy a request for information.
  - Example: A hospital employee leaves a voicemail message detailing a patient's diagnosis and care plan, when a request to return the call would have been sufficient.
- Failing to obtain an individual's valid authorization when one is required.
  - Example: A hospital executive discloses a patient's PHI in response to an inquiry from a reporter.

Questions?