The Basics of HIPAA Privacy and Security and HITECH

Protecting Patient Privacy

Disclaimer

• The content of this webinar is to introduce the principles associated with HIPAA and HITECH regulations and is not intended to serve as an annual employee training or as a conclusive education on HIPAA laws. Each HIPAA entity should personalize their own employee training and should undergo thorough HIPAA training in accordance with their HIPAA compliance plan.

• Additional information regarding the HIPAA law can be found on the official U.S. Department of Health & Human Services website. A summary of this law can be found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
Objectives

- Become familiar with HIPAA regulations and the requirements for compliance
- Understand HITECH regulations and how they apply to compliance in your practice
- Awareness of expectations for compliance and consequences of non compliance
- Know how to properly respond to concerns

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- **HIPAA Privacy** – Protection for the privacy of Protected Health Information (PHI)
- **HIPAA Security** – Protection for the security of electronic Protected Health Information (e-PHI)
What is the difference between Privacy and Security?

- The **Privacy Rule** sets the standards for how to maintain the privacy of personal information in all of its forms. It’s focus is on overall confidentiality.

- The **Security Rule** defines the standards for safeguards of personal information specifically related to electronic PHI (e-PHI).
  - Successfully privacy rule will depend on a good implementation of the security rule.

Who Does This Law Apply To?

 Individuals, organizations, and agencies that meet the definition of a **covered entity** under HIPAA must comply with the Rules’ requirements to **protect the privacy and security of health information** and must **provide individuals with certain rights** with respect to their health information. If an entity is not a covered entity, it does not have to comply with the Privacy Rule or the Security Rule.
Covered Entities

A covered entity is a

- healthcare provider,
- a health plan,
- healthcare clearing house

.....who transmits any health information in electronic form

### Health Care Provider
- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

......if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

### A Health Plan
- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs

### Clearinghouse
- Includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

http://www.cms.gov/HIPAAGenInfo/06_AreYouACoveredEntity.asp
Business Associates

• A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity but is not part of that entity.
• A person or business is NOT a “business associate” if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. (i.e. janitor, building maintenance, tax accountant, etc)

Privacy Rule

Protected Health Information is:

• Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
  – The individual’s past, present or future physical or mental health
  – Health care services provided to the individual
  – Payment for health care services
• Includes all demographic information that identifies or can be used to identify the individual.
Examples of PHI

- Name
- Address (including street, city, county, zip code and equivalent geocodes)
- Name of employer
- Any date (birth, admit date, discharge date)
- Telephone and Fax numbers
- Electronic (email) addresses
- Social Security Number
- Medical Records

Permitted Disclosure of PHI

- **Individual** who is the subject of information

**TPO** – Treatment, Payment, Operations:
- **Treatment**- coordination of care between one or more health care providers
- **Payment**- activities required to bill and collect for health care services provided to the patient.
- **Operations**- includes business management and administrative activities, quality improvement, billing, collections, audits, and training
Principle of Minimum Necessary

- A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. (i.e. If the whole medical record is not needed to fulfill the request, then only send the parts that are needed)

Minimum Necessary is **NOT** required for the following:
- Requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Disclosures made pursuant to an individual’s authorization.
- Disclosures to the Department of Health and Human Services (HHS)
- Uses or disclosures that are required by other law

Notice of Privacy Practices (NPP)

- HIPAA requires each entity to
  1. Provide each patient a copy of their NPP that describes
     - how a covered entity may use or disclose (PHI),
     - what the patient’s rights are and
     - what the covered entity’s obligations are with respect to that information.
  2. Request acknowledgement of receipt from the patient
     - Acknowledgement can be done in a variety of formats
     - The patient signs a statement that they have received or been given access to the entities NPP.
  3. Post the NPP at each site in a clear and prominent place and on the website if one exists.
Is the Patient Required To Sign The NPP?

• The law does not require patients to sign the “acknowledgement of receipt of the notice” in order to receive services.
• If the patient refuses to sign the acknowledgement, the provider must note that it was offered and refused.
• In an emergency situation, delivery of the NPP and acknowledgement is not required prior to delivering services but should be done after.

  *Signing the acknowledgement does not mean that the patient agrees to any special uses or disclosures of his or her health records.*

Other Uses and Disclosures of PHI

• Written authorization for any use or disclosure of protected health information that is not for TPO or otherwise permitted. (life insurance, employers, research, marketing, etc)

• The authorization should
  – Describe the PHI to be used or released
  – Identify who may use or release the PHI
  – Identify who may receive the PHI
  – Describe the purposes of the use or disclosure
  – Identify when the authorization expires
  – Be signed by the patient or someone making health care decisions (personal representative) for the patient
Patients Rights

• The right to request alternative forms of communications (mail to P.O. Box instead of street address, no message on answering machine, etc.)
• The right to access and copy patient’s PHI
• The right to an accounting of the disclosures of PHI
• The right to request restriction of PHI uses & disclosures
• The right to request amendments to information

Basics for Protecting PHI

• Look at a patient’s PHI only if you need it to perform your job
• Use a patient’s PHI only to the extent that is required to perform your job
• Give a patient’s PHI to others only when it’s necessary for them to perform their jobs
• Talk to others about a patient’s PHI only if it is necessary to perform your job, and do it discreetly
• Reasonable standards for different groups
Privacy Administrative Requirements

- Develop and implement written privacy policies and procedures
- Designate a privacy official
- Train all workforce members on privacy policies and procedures
- Have and apply appropriate discipline against employees who violate privacy policies and procedures
- Safeguard PHI
- Maintain all HIPAA documents for a period of 6 years

Privacy Rule Summary

- Using PHI for TPO and other authorizations
- Securing PHI so as not to be readily available to those who do not require access
- Notifying patient about his or her privacy rights and how their information can be used
- Adopting and implementing privacy policies and procedures and designating a privacy officer to oversee
- Training employees so that they understand these privacy procedures
HIPAA Security Rule

- The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information “electronic protected health information” (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

HIPAA Security Safeguards

- Administrative Safeguards
  - Security management process
  - Information access management
  - Workforce training, management and evaluation
- Physical Safeguards
  - Facility access and control
  - Workstation and device security
- Technical Safeguards
  - Access controls
  - Audit controls
  - Integrity controls
  - Transmission security
Basic Security Guidelines

• **Secure logins and Passwords** – each person who accesses PHI should have their own unique user ID and password. Passwords should be kept confidential and not shared with anyone else. Passwords should be changed periodically.

• **Email encryption** – all emails with PHI should be secured with encryption and include a confidentiality statement within the email.

• **Workstation security** – lock up systems when not being used, log off when leaving a computer, encrypt information stored on the computer, and use screen savers when stepping away.

• **Disaster Controls** – protect systems against hazards or natural disasters, locate above ground, surge protectors

• **Malware** – protect against viruses, spyware, and worms that could compromise security, avoid suspicious email

90/10 Rule

Remember

- 10% of security safeguards are technical
- 90% of security safeguards rely on the computer user to adhere to good computing practices
HITECH

- **Health Information Technology for Economic and Clinical Health Act**

- HITECH is a part of the American Recovery and Reinvestment Act of 2009 (ARRA)
- It is a federal law that affects the healthcare industry
  - Allocated ~$20 billion to health information technology projects
  - Expanded the reach of HIPAA by extending certain obligations to business associates
  - Imposed a nationwide security breach notification law
  - Added teeth to enforcement

What is a Breach?

- Only applies to unsecured PHI

1. Use or disclosure of the patients PHI that is not permitted under the privacy rule
2. The use or disclosure compromises the security or privacy of the patient’s PHI

- If there is not a risk of significant financial, reputational or other harm to the individual whose PHI was used or disclosed it is not considered a HITECH breach but a violation of the Privacy Rule
Breach Notification

• A major portion of the HITECH law that is currently in effect!

• The law requires covered entities and business associates to notify the following in the event of a breach with 60 days
  – individuals,
  – the Secretary of Health and Human Services,
  – the media (if breach affected over 500 people)

• There are exceptions

Components of the notification must include;
  – A description of the breach,
  – a description of the types of information that were involved in the breach,
  – the steps affected individuals should take to protect themselves from potential harm,
  – a brief description of what the covered entity is doing to investigate the breach, mitigate the potential harm, and prevent future breaches from occurring,
  – provide contact information for the covered entity.

Additional information can be found on HHS website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
Examples of PHI Breaches

- An employee is curious about his or her favorite professional football quarterback who is a patient at the practice or hospital and accesses the patient’s medical record then shares with friends.
- An unencrypted thumb drive containing PHI is left in a car and the car is stolen.
- PHI is faxed to the wrong number outside of the covered entity.
- PHI has been changed or destroyed in an unauthorized manner.

Enforcement

- HHS will be conducting audits of Covered Entities and Business Associates to ensure their compliance with the Privacy and Security Rules (this is already happening)
- Covered entities and individuals may be subject to civil money penalties. Maximum raised from $25,000 to 1.5 Million per year
- HITECH expanded ability to impose criminal penalties for violations
- No longer can parties avoid penalties by claiming that they did not have actual or constructive knowledge of the violation
- Regulations will be issued permitting portions of financial recoveries for HIPAA violations to be paid by HHS directly to individuals harmed by the violation
FAQ

HHS website provides answers to many frequently asked questions regarding HIPAA privacy and security.

http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html

Test What You’ve Learned

1) The Notice of Privacy Practices (NPP) must be:

A. Offered to each patient at the first visit after April 14, 2003
B. Posted on my website, if I have one
C. Posted in the office
D. All of the above
Test What You’ve Learned

1) The Notice of Privacy Practices (NPP) must be:

A. Offered to each patient at the first visit after April 14, 2003
B. Posted on my website, if I have one
C. Posted in the office
D. All of the above

Answer: D  The NPP must be offered to every patient, posted on the website and posted in a prominent place at each site.

Test What You’ve Learned (continued)

2) When a patient requests access to his/her medical records:

A. I always have to provide them a complete copy
B. I can provide a summary if I think it is too difficult for the patient to interpret or if information may be deemed harmful
C. I can charge a reasonable fee for copying and postage
D. B and C
2) When a patient requests access to his/her medical records:

A. I always have to provide them a complete copy
B. I can provide a summary if I think it is too difficult for the patient to interpret or if information may be deemed harmful
C. I can charge a reasonable fee for copying and postage
D. B and C

Answer: D  Information such as psychotherapy notes, information compiled for legal proceedings, and laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access may not be granted to a patient. A reasonable cost based fee may be charged.

3) Protected health information (PHI) can ONLY be given out after obtaining written authorization.

A. True
B. False
3) Protected health information (PHI) can ONLY be given out after obtaining written authorization.

A. True
B. False

Answer: B  False- PHI can be given out for Treatment, Payment, or Operations

4) If a patient wants to request a restriction on the disclosure of his/her protected health information (PHI):

A. The covered entity must agree to it
B. It must be in writing
C. Can be retroactive to cover information already released
D. The patient can not restrict disclosure of his PHI
4) If a patient wants to request a restriction on the disclosure of his/her protected health information (PHI):

A. The covered entity must agree to it
B. It must be in writing
C. Can be retroactive to cover information already released
D. The patient can not restrict disclosure of his PHI

Answer: B  This request must be in writing, will apply to all future disclosures, and the entity must consider and comply with the request unless superseded by other federal or state law.

5) I don't have to worry about the minimum necessary requirement for:

A. Disclosures to or requests by a health care provider for treatment
B. Uses or disclosures made pursuant to an authorization
C. Uses or disclosures made to the individuals family
D. Disclosures made to the Secretary of Health and Human Services (HSS), pursuant to the stated rules
E. All of the above
F. A, B, and D only
Test What You’ve Learned (continued)

5) I don’t have to worry about the minimum necessary requirement for:

A. Disclosures to or requests by a health care provider for treatment
B. Uses or disclosures made pursuant to an authorization
C. Uses or disclosures made to the individuals family
D. Disclosures made to the Secretary of Health and Human Services (HSS), pursuant to the stated rules
E. All of the above
F. A, B, and D only

Answer: F  Complete record information may be released to another health care provider for treatment, pursuant to an authorization from the patient, or as required by HHS.

Test What You’ve Learned (continued)

6) I don’t need a business associate agreement for:

A. My employees
B. My cleaning service
C. Independent entity providing medical chart audits for my practice
D. Contracted employees such as a physical therapist who perform a substantial portion of their work at my practice
E. None of the above
F. A, B, and D only
6) I don’t need a business associate agreement for:

A. My employees  
B. My cleaning service  
C. Independent entity providing medical chart audits for my practice  
D. Contracted employees such as a physical therapist who perform a substantial portion of their work at my practice  
E. None of the above  
F. A, B, and D only  

Answer: F  
Business Associate agreements are not required for employees or other entities not involved in the use or disclosure of protected health information.

7) A privacy officer should conduct the following steps:

A. Identify the internal and external risks of disclosure of protected health information (PHI)  
B. Create and implement a plan to reduce the risk of releasing PHI in those areas identified  
C. Train all personnel on the practice’s privacy and security of PHI  
D. Monitor the implementation and enforce appropriately any breaches of policy  
E. All of the above  
F. A, B, and D only
Test What You’ve Learned (continued)

7) A privacy officer should conduct the following steps:
A. Identify the internal and external risks of disclosure of protected health information (PHI)
B. Create and implement a plan to reduce the risk of releasing PHI in those areas identified
C. Train all personnel on the practice’s privacy and security of PHI
D. Monitor the implementation and enforce appropriately any breaches of policy
E. All of the above
F. A, B, and D only

Answer: E  A privacy officer should conduct all of these steps

Test What You’ve Learned (continued)

8) Within a clinic, a human resource manager receives and opens an e-mail containing PHI about a patient which a medical assistant mistakenly sent to her. The human resource manager deletes the email and alerts the medical assistant.

Does this constitute a breach under the HITECH rule?
8) Within a clinic, a human resource manager receives and opens an e-mail containing PHI about a patient which a medical assistant mistakenly sent to her. The human resource manager deletes the email and alerts the medical assistant.

Does this constitute a breach under the HITECH rule?

Answer: NO  The HR manager unintentionally accessed PHI to which she was not authorized to have access. However, the HR manager’s use of the information was done in good faith and within the scope of authority, and therefore, would not constitute a breach and notification would not be required, provided the employee did not further use or disclose the information accessed in a manner not permitted by the Privacy Rule.

www.hhs.gov

This presentation has covered the basics of the HIPAA privacy and security rules and components of the HITECH law with emphasis on protecting Protected Health Information under the guidance of the US Department of Health and Human Services, Division of Office for Civil Rights.

For more information go to http://www.hhs.gov/ocr/privacy/.