HIPAA TRAINING

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA

- HIPAA Privacy and Security Rules
- HITECH
- Breach
- Enforcement, Fines, and Penalties

HIPAA PRIVACY SECURITY BREACH

- Identify important definitions associated with HIPAA rules and regulations
- Describe permitted uses and disclosures
- Describe Notice of Privacy Practices (NPP)
- Identify patient rights
- Identify ways to protect patient information
- Discuss process for documentation of a privacy complaint

QUIZ-HIPAA BASICS

- Having a patient sign in when they arrive for an appointment is allowable.
- A. True
- B. False

- Answer: A

QUIZ

- A single piece of paper with a patient's name on it can be thrown in the regular trash.
- A. True
- B. False

- Answer: B

QUIZ

- Leaving normal test results on an answering machine is acceptable without patient's authorization.
- A. True
- B. False

- Answer: B

QUIZ

- Clinical staff may share logins and passwords to save time when accessing patient information stored electronically.
- A. True
- B. False

- Answer: B

QUIZ

- If a patient requests a copy of their entire medical record, all records, even if they came from another healthcare provider must be released.
- A. True
- B. False

- Answer: A

QUIZ

- Workers must only look or access information on patients in which they are involved in the care.
- A. True
- B. False

- Answer: A

QUIZ

- Information about patients receiving care in a facility should not be shared on a personal social media site.
- A. True
- B. False

- Answer: A

HIPAA ENACTMENT

- The Privacy Rule, which is a Federal law, outlines how healthcare providers can use information to provide patient care. It also established certain patient rights regarding how their health information is used. The Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral.
- The Security Rule is also a federal law and protects health information in electronic form. The law requires healthcare providers and others covered by HIPAA to ensure that electronic protected health information is secure.

DEFINITIONS

- **Health and Human Services (HHS)-**governments principal agency for protecting the health of all Americans
- **Office for Civil Rights (OCR)-**oversees and enforces the Privacy and Security rules
- **Covered Entity (CE)-**a healthcare provider who performs identified transactions electronically. For example, billing for provided services electronically.
- Protected Health Information which includes both financial and healthcare information (PHI)

DEFINITIONS

- Electronic Protected Health Information (ePHI)
- **Business Associate (BA)-**an entity who performs a task for a covered entity utilizing protected health information provided by that covered entity. Subcontractors of business associates may also be included in this definition.
- **Use-**Sharing, application, utilization of protected health information within the entity (facility) which holds the information
- **Disclosure-**Release, transfer, provide, allowing of access, to any entity (person or facility) outside of the entity (facility) holding the information

DEFINITION OF PHI

- Protected Health Information (PHI) is information that relates to:
  - The individual's past, present, or future physical or mental health or condition
  - The provision of health care to the individual, or
  - The past, present, or future payment for the provision of health care to the individual,
- PHI which is often referred to as individually identifiable health information includes items such as: name, address, birth date, and social security number.

QUIZ

- Which of the following items are considered protected health information?
- A. geographic subdivisions smaller than a state
- B. vehicle identifiers and serial numbers including license plates
- C. device identifiers and serial numbers
- D. e-mail address
- E. internet protocol addresses

- Answer: A, B, C, D, E

PHI

- Names
- All elements of dates (except year) related to an individual (including dates of admission, discharge, birth, death, and for individuals over 89 years old, the year of birth must not be used.
- Telephone numbers
- Fax numbers
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Biometric identifiers (including finger and voice prints)
- Full face photos and comparable images
- Any unique identifying number, characteristic or code

QUIZ-COVERED ENTITY

- A covered entity (CE) may use or disclose medical records for treatment purposes.
- A. True
- B. False

- Answer: A

COVERED ENTITY

- A CE may use or disclose healthcare information for treatment purposes. They may also utilize this information for payment, and healthcare operations after providing a Notice of Privacy Practices (NPP).

QUIZ

- When releasing health information the amount of information needed to complete the request should be provided.
- A. True
- B. False

- Answer: A

QUIZ

- As a healthcare provider, it is acceptable to review records of anyone seeking care in the facility; including your neighbor's recent visit.
- A. True
- B. False

- Answer: B

TPO (TREATMENT, PAYMENT, HEALTHCARE OPERATIONS)

- Consultation between healthcare providers -T
- Billing and collection activities -P
- Reviewing competence or qualifications of healthcare providers -HO
- Referral of a patient from one healthcare provider to another -T
- Providing, coordinating or managing care -T
- Case management -HO
- Training healthcare and non-healthcare personnel -HO

NOTICE OF PRIVACY PRACTICES (NPP)

- A Notice of Privacy Practices outlines how patient information can be used and disclosed by your facility. It also outlines certain rights of patients related to how their information is utilized.
- The following are important reminders about the Notice of Privacy Practices.
  - Each new patient must be offered a copy of the NPP
  - Each patient should sign that they have been offered the NPP
  - If the patient refuses to sign, the employee should document that the NPP was offered
  - The NPP must be visibly posted in a common patient area such as the waiting room and on any facility website

PATIENT RIGHTS-ACCESS

- Every patient has the right to review and obtain a copy of their protected health information.
  - Medical or dental information created during the delivery of care
  - Financial information

PATIENT RIGHTS-AMENDMENT

- Every patient has the right to request an amendment of their PHI in a designated record set. The request should be in writing. The decision on whether or not to amend the information is made by the provider involved in the delivery of care.
- For example: the patient reports they have 4-5 alcoholic beverages each week and the record reflects the patient has 4-5 alcoholic drinks each day. The patient may ask for the record to be amended to correct the entry

PATIENT RIGHTS-DISCLOSURE ACCOUNTING

- Every patient has the right to an accounting of the disclosures of their protected health information by their healthcare provider or business associate. This accounting provides information to the patient about certain disclosures of their health information that they may not be aware of.
- For instance, reporting of a communicable disease is required by law. Since required by law, the patient is not notified of the reporting process therefore is not aware the report is made. This disclosure would be recorded on an Accounting of Disclosures log.

PATIENT RIGHTS-RESTRICTION REQUEST

- Every patient has the right to request a restriction on the release.
- Examples include:
  - The patient may ask that insurance not be filed for lab tests drawn during a visit. This is the only restriction that MUST be accepted by the facility.
  - The patient must agree to pay for the services out of pocket.
  - The patient may request that their cancer diagnosis is not discussed with their children
  - The patient may request that certain staff in the clinic not have access to their health records

PATIENT RIGHTS-CONFIDENTIAL COMMUNICATIONS

- Every patient has the right to request confidential communications.
- An example would be contact the patient at a specific address or phone number

INCIDENTAL USE AND DISCLOSURE

- **Which of the following are incidental disclosures which are allowed under the Privacy Rule?**
- 1. Nurse Nancy calls the patient back to the exam area by saying, 'Mrs. Smith the doctor is ready to begin your skin biopsy.'
- 2. Nurse Nancy calls Mrs. Smith by name in the reception area as she escorts her to the patient care area.
- 3. Reception personnel quietly confirm home address and phone number with a patient checking in.
- 4. Patient name and appointment time on a sign in sheet.
- 5. Leaving an appointment reminder with only a limited amount of information on a home answering machine. Care should be taken not to leave sensitive information as part of the message.
- 6. Patient name, appointment time, and reason for visit on a sign in sheet.

- Answer: 2, 3, 4, 5

RELEASE OF INFORMATION

- Outside of treatment, payment, or healthcare operations, or as required by law, a HIPAA compliant authorization is required for use or disclosure of health information. A valid authorization which is signed by the patient MUST accompany the request.
- The following items must be stated on an authorization request:
  - Who will receive the PHI
  - The patient's signature
  - Description of the purpose of the release which can be stated as 'at the request of the patient'
  - Statements outlining patient rights related to the authorization
  - Expiration date or event
  - Who is releasing the PHI
  - Description of the PHI to be released

QUIZ

- A CE may release protected health information (PHI) to the individual only.
- A. True
- B. False

- Answer: B
- If the patient signs a HIPAA compliant authorization form the CE must release the requested information as requested by the patient. For example, this request may be to release information to another person, attorney, or a life insurance company.

QUIZ

- With the proper authorization, protected health information may be released to friends and family of the patient.
- A. True
- B. False

- Answer: A
- A signed HIPAA compliant authorization is required for release of protected health information. At times a patient may be accompanied by another person during the exam. It is best to seek the verbal permission of the patient prior to discussing their health information. This is referred to as informal approval. If there is an emergency situation and if the healthcare provider feels it is in the best interest of the patient, pertinent information may be shared with friends or family involved in the patient's care.

QUIZ

- In order to release information to an attorney, a signed authorization is not required.
- A. True
- B. False

- **Answer: B**
- A signed authorization from the patient is required even if the request from the attorney is on behalf of the patient.

PROTECT PATIENT INFORMATION

- Protection of a patient's health information is a key part of the healthcare provider's role. Everyone involved in delivery of healthcare services should remember the following safety measures:
  - Discuss sensitive issues in a private location
  - Access, discuss, or release the minimum amount of information needed to complete a task
  - Ensure the patient's permission is obtained prior to discussing their healthcare with others such as a spouse, child, or parent
  - Secure printed information such as faxes, schedules, and test results when left unattended
  - Use approved forms of release for patient information
  - Shred paper documents, or any other storage media prior to disposal to prevent inappropriate disclosure

PROTECTING PATIENT PRIVACY

- Acceptable/Not Acceptable
- 1. This message is for Ms. Levi, your HIV test results were questionable. Please give us a call at the office
- 2. Mrs. Smith arrives for her appointment and the receptionist asks her to sign in and have a seat. The sheet asks for her name and arrival time.
- 3. While waiting to speak with the doctor, Beverly, a family member, was able to see patient information on a computer screen. She saw that her neighbor was being treated for recurrent bloody stools.
- 4. Nancy Nurse enters the waiting area and calls Patty Patient back for her visit with the doctor.

- **Answer: 2, 4**

PROTECTING PATIENT PRIVACY

- Acceptable/Not Acceptable
- 5. Bob, the radiology technician posts on his Facebook, "Billy Bob screamed the entire time I took his x-rays. Kids are a pain!"
- 6. As Bob Barker checks in, the receptionist quietly confirms his current address and phone number
- 7. All staff check their work space to ensure protected health information is secured to limit the amount of information housekeeping staff may see when cleaning the office.

- Answer: 6, 7

COMPLAINT DOCUMENTATION

- All complaints associated with privacy and security of patient information must be documented and investigated. A patient calls the facility and voices a complaint that normal lab results were left on their home answering machine.
- 1. Forward the complaint to responsible person at the facility. This is usually the Privacy or Security Officer.
- 2. Complaint is documented
- 3. Complaint is investigated by speaking with the person lodging the complaint as well as any workers involved in the situation.
- 4. Based on investigation, sanctions may be required for workers involved if established policies and procedures have not been involved.
- 5. Follow-up with the patient should occur to discuss the complaint, the results of the investigation, and to provide closure for the patient.
- 6. Additional employee training and an update to current practices may be indicated based on the results of the investigation.

COMPLAINTS

- These are the complaints made to Health and Human Services, Office for Civil Rights, based on the order of frequency:
- 1. Impermissible uses and disclosures of protected health information
- 2. Patient information not properly protected
- 3. Denial of patient access to their records
- 4. Release of more information than necessary or not following the minimum necessary standard.

QUIZ

- Any friend or family member of a patient can walk into a healthcare facility and obtain a copy of the patient's medical records.
- A. True
- B. False

- Answer: B

QUIZ

- It is appropriate to leave normal test results on a patient's voice mail at work even without written authorization.
- A. True
- B. False

- Answer: B

QUIZ

- If a complaint is voiced related to the privacy or security of patient information what should be done?
- A. Nothing, the patient just doesn't understand the HIPAA rules
- B. Investigate the complaint
- C. Fire the healthcare worker involved on the spot.

- Answer: B

SECURITY

- Describe why protection is needed for PHI stored electronically or ePHI
- Describe what ePHI should be protected
- Identify potential locations of ePHI
- Discuss best practices for password protection
- Describe methods to protect information stored electronically
- Identify security incidents

EPHI SECURITY PROTECTION

- The Security Rule identifies measures to protect health information stored electronically to ensure it is available for use to provide healthcare services.
- What are examples of situations which can impact the integrity or destroy ePHI?
- A. Natural disasters or a fire
- B. Accidental or intentional destruction by staff or business associates
- C. Theft of computer hardware, servers, etc. storing ePHI
- D. Unauthorized access of ePHI by hackers, stolen passwords or by employees

- Answer: A, B, C, D

LOCATION OF EPHI

- It is important to remember any health information in electronic format must be protected against unauthorized access, use, or disclosure. Listed below are devices on which ePHI may be created, accessed, or stored.
  - Servers, patient care equipment requiring data entry of patient info, back up devices (hard drives, CDs, tapes), fax/copy machines, thumb or flash drives, smart/mobile phones, laptop, tablets, or desktop computers
- PHI may also be sent electronically for example for billing purposes or transcription services. Protected health information may also be faxed, e-mailed, and backed-up to a remote site through an electronic transfer. Any transmission of health information must be done in a secure manner.

EPHI PROTECTION

- One benefit of having healthcare information in an electronic format is the ability to easily communicate and share patient records with others in the healthcare community involved in the care of the patient. But to ensure accessibility of accurate information certain protections must be in place.

EPHI PROTECTION

- **Measures to ensure protection of ePHI include the following:**
- Individual login and password for every employee or vendor who may access protected health information
- Log off or lock computer when leaving work stations even if stepping away for a short period of time.
- Automatic logoff if system left unattended for designated period of time.
- Antivirus software to prevent system exposure to virus attacks
- Audits of access to information stored electronically. These audits may show inappropriate access of protected information.
- Encryption of data stored electronically
- Building security to reduce the likelihood of theft. This may include the use of an alarm system.

PASSWORD PROTECTION

- Must use at least one capitalized letter
- Must use at least one number
- Must be between 6 and 20 characters
- Is not a commonly used password

INTERNET AND VIRUS PROTECTION

- Inappropriate use of the internet can lead to issues such as virus entry into a computer or network in your facility. A virus can compromise the integrity of information and potentially make it unavailable for use in the delivery of patient care services.
- Follow these safety tips on internet use:
  - Access information only on approved internet sites from work computers
  - Open emails and attachments from reliable sources
  - Do not download/upload programs without management approval
  - Internet access should be limited to sites approved by management
  - Avoid accessing social networking sites for personal use when using work computers
  - Do not open email or click on links from social media sites as this may lead to inappropriate access into your facility's system(s)

ELECTRONIC PROTECTION

- **Acceptable**/Not Acceptable
- The administrator was late leaving work for her son's baseball game and to save time didn't log off or lock her computer.
- The new receptionist didn't have a password to the electronic medical record system, so the administrator shared hers.
- An accident victim came in for treatment and a staff member took a photo with her cell phone and posted the image on Facebook with the text, "Don't text and drive."
- **A gentleman came to the practice with a HIPAA compliant authorization requesting a copy of his wife's medical records. After confirming signature of the patient, the records were released.**

ELECTRONIC PROTECTION

- ALWAYS:
  - Log off or lock computer when walking away from work station
  - Create a strong password
  - Access only information on patients in which you are involved in the delivery of care
  - Be aware of your company policy on internet and social media access from work equipment
- NEVER:
  - Post comments about patients on any type of social media
  - Take pictures of patients on your smart phone for personal use
  - Never disclose medical information to people not approved by the patient

SECURITY INCIDENTS

- System Failure
- Server stored in a secure place with limited access
- Improper use or disclosure of information
- Theft of server, computers, etc.
- Unauthorized access
- Unauthorized data changes
- Individual login and passwords for all employees and vendors
- Use of anti-virus on all network computers
- Natural disaster
- Virus

- Non Event
- Security Event

QUIZ

- It is a recommendation that employees not access social media sites from work computers.
- A. True
- B. False

- Answer: A

QUIZ

- Sharing your password with your coworker in case she/he needs to access your computer is an acceptable process.
- A. True
- B. False

- Answer: B

QUIZ

- Which of the following is the best choice for a password?
- A. Password1
- B. Workstation2
- C. !Jones01
- D. @jk92BMC

- Answer: D

HITECH

- Describe impact of HITECH on covered entities and business associates
- Define breach
- Identify possible breach scenarios
- Describe the procedure for reporting an incident which may be a breach
- Describe the impact of a breach
  - Patient
  - Employee
  - Facility

HITECH IMPACT

- The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law on February 17, 2009 to protect and promote meaningful use of health information technology
- As a result of the changes to both the privacy and security rules, more stringent safeguards are now required to protect health information.
- Two very important elements of the Act:
  - The term BREACH was defined
  - Business associates just like your facility, must comply with many elements of the privacy and security rules

BUSINESS ASSOCIATE

- A business associate is a person or entity which creates, receives, maintains, or transmits protected health information on behalf of your practice or facility.
- Because of their access to PHI, business associates and their subcontractors must have policies and procedures in place, provide training to their employees and must report any potential breach scenarios to you, the covered entity

IDENTIFYING BUSINESS ASSOCIATES

- Transcription Services
- Billing Company
- IT Company
- Collections Agency

- Non business associates
  - Pharmaceutical Reps
  - Cleaning staff

BREACH

- An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information.
- Examples:
  - Theft of server/desktop computer (patients impacted: 3,500)
  - Loss of laptop computer (patients impacted: 812)
  - Hacking/IT incident (patients impacted: 2,300)
  - Loss of portable electronic device (patients impacted: 19,222)

BREACH INCIDENTS

- Which of the following represent possible breach scenarios?
- A. Loss of power to the building, resulting in the computers being down.
- B. An employee or business associate downloads a link from an email sent by a friend, inadvertently downloading a virus.
- C. An employee or business associate with authorized access to PHI, reviews her friend's recent visit to the facility.
- D. A thumb/flash drive containing copies of patient visit notes and x-ray images is misplaced. The thumb/flash drive was encrypted. (HHS has determined that if information is protected through an acceptable encryption process and the information is lost or inappropriately accessed it is not considered a breach)

- Answer: B, C

REPORTING INCIDENTS

- Step 1: Report the incident to the Privacy or Security Officer
- Step 2: Management will complete the investigation and determine if the event is a breach.
- Step 3: If the event is determined to be a breach, the patient must be notified within 60 days of discovery of the incident.
- Step 4: If 500 patients or more are impacted by the breach in the same state, both the local media and HHS must be notified at the same time as patient notification occurs

- A breach can have far reaching implications, both from a financial and reputational perspective

BREACH IMPACT

- Patient
  - Misuse of personal data
  - May become a victim of identity theft
- Facility
  - Loss of integrity of data
  - Damaged reputation and loss of trust in the healthcare community
  - Negative press
  - Penalties, fines, and lawsuits

BREACH PROTECTION

- **Risks**

- Transporting health information in personal vehicles which are not secured in some manner
- Posting information about a patient on social media sites
- Looking at your neighbor's health records to determine the reason for recent health care

- **Prevent**

- Ensuring the correct mailing address is utilized when sending out mail to a patient
- Accessing only the information needed to complete a task
- Protect any info stored electronically, especially on portable devices such as a laptop or thumb/flash drive through an encryption process
- Programming frequently used numbers into the fax machine(s) at your site

QUIZ

- The first step in a potential breach situation is to:
- A. Try to cover it up
- B. Report it to proper administration
- C. Determine the fine and penalty

- Answer: B

QUIZ

- If a breach is determined, the patient doesn't have to be notified.
- A. True
- B. False

- Answer: B

QUIZ

- If _____ or more patients are impacted by a breach the local media must be notified.
- A. 200
- B. 350
- C. 500
- D. 750

- Answer: C

ENFORCEMENT, FINES, AND PENALTIES

- Identify changes in fines and enforcement as a result of HITECH

FINES

- HITECH changed the level of fines and penalties which can be assessed to individual facilities and individual employees
  - Fines can range from $100 to $1.5 million
  - Willful neglect can lead to a fine of $1.5 million
  - The facility and its business associates are subject to all fines and criminal charges
  - Employees may now face criminal penalties which can include time in prison
  - Increase in enforcement and fines by HHS

ENFORCEMENT

- How has HHS increased enforcement activity? Select all that apply.
- A. Random audits of individual facilities
- B. Investigation of complaints related to non-compliance with HIPAA Privacy and Security Rules
- C. Monitoring and investigation of breaches impacting over 500 individuals which are reported.

- Answer: A, B, C

QUIZ

- As a result of the HITECH ACT, enforcement activities have increased. Facilities and their business associates are facing the possibility of increased fines if found they are not adequately protecting patient information.
- A. True
- B. False

- Answer: A

QUIZ

- HIPAA Privacy vs. HIPAA security
- 1. Discussing a patient while having dinner with friends at a local restaurant
- 2. Mailing sensitive lab results to the wrong address
- 3. Releasing health information to a life insurance company without a HIPAA compliant authorization
- 4. Sharing a login and password with a co-worker, which the co-worker uses to access information inappropriately
- 5. A break-in occurs and 3 laptop computers containing patient information are stolen

END!