Assessing Your Pharmacy’s HIPAA Policies & Procedures

Presented by:
Craig M. Burridge, M.S., CAE
CEO
South Carolina Pharmacy Association
Learning Goals & Objectives

- Identify the *Laws covering confidentiality* and their lead up to HIPAA
- Recognize the *Standard Principles governing confidentiality* as it relates to ‘patient records’
- Identify the need for and responsibilities of a ‘privacy officer’ and ‘workforce training requirements’
- Differentiate between the proper ‘uses and disclosers’ of ‘protected health information’ and ‘permitted uses and disclosures’
Learning Goals & Objectives

- Recognize when ‘authorization’ is necessary for ‘protected information’
- Identify the requirements for the ‘distribution of Privacy Practices Notices’
- Know how to develop an ‘electronic protected health information’ policy
- Recognize how to ‘mitigate’ and ‘notify’ affected individuals in case of a breach of protected health information
- Identify the ‘expanded’ HIPAA requirements under the Health Information Technology for Economic and Clinical Health Act “HITECH”
Laws Governing Confidentiality

• Freedom of Information Act:
  – *Provided a means for private citizens to access information related to federal agencies*;
  – *Only applied to hospitals included in the VA and DoD systems*;
  – *Exempted certain medical records*. 
Laws Governing Confidentiality

• The Privacy Act of 1974:
  – Provided *protection to private citizens* from information gathered by the federal government;
  – Limited the *scope and use of confidential data* lawfully collected by federal agencies;
  – Allowed federal agencies to gather information for ‘*needed use;*’ (i.e. IRS)
  – *Limited* how a *federal agency shared its information* with other like agencies.
Laws Governing Confidentiality

• The Medicare Act:
  – *Required all participating entities to maintain the confidentiality of its medical records.*

• HIPPA: *Health Insurance Portability and Accountability Act of 1996* – “*Provides guidance to individuals within a company who ‘have’ or ‘need’ access to protected health information*”
Laws Governing Confidentiality
- New -

• The *Health Information Technology for Economic and Clinical Health Act* ("HITECH") – aka – “Omnibus Rule”
  – Released originally on January 17, 2013;
  – *Expands the reach of* the *Breach Notifications Rules*;
  – Omnibus Rule **effective march 26, 2013**;
  – Covered entities have until **September 23, 2013** to come into compliance.
HIPAA Monetary Penalties

• Monetary Penalties for Violations:
  • Penalties range from a ‘minimum’ of $100 per violation ($25,000 per year) to a ‘maximum’ of $50,000 per violation ($1.5 million per year) for violations committed without knowledge and without reason to know;

  • Penalties of a ‘minimum of $50,000 per violation ($1.5 million per year) with no set ‘maximum’ amount for ‘willful neglect’ violations.
Standard Principles Governing Confidentiality
“Patient Records”

- State laws, regulations, accreditation standards and industry guidelines all reinforce the requirement that “health care providers **MUST** maintain detailed records and documentation for all patients.”

- All **HIPAA Policies and Procedures** dealing with documentation and maintenance of patient health records **MUST** have the following elements:
  
  - Detailed guidelines as to ‘**what**’ patient information is ‘**added**’ to patient records;
  - Instructions as to the ‘**length of time**’ these records are maintained;
  - Step by step instructions on ‘**how**’ these records are to be disposed of and destroyed.
Privacy Officer

• Every pharmacy should designate someone as their ‘privacy officer.’

• Responsibilities of the Privacy Officer:
  – *Implementing the pharmacy’s ‘Privacy Policy & Procedures;’*
  – *Developing related forms and manuals;*
  – *Providing information to individuals concerning the pharmacy’s privacy policies & procedures (training); and*
  – *Receiving and handling complaints concerning the pharmacy’s privacy policies & procedures (both external and internal)*
Privacy Officer

• Workforce Training:
  
  – *Upon hiring, and annually thereafter*, the pharmacy’s ‘privacy officer’ (or other designee) *will train* all employees ‘who have access to protected health information’
  
  – Training will cover your staff’s *responsibilities* under the pharmacy’s ‘privacy policies & procedures’ and HIPAA including:
    
    • HIPAA *Privacy Rule*;
    • HIPAA *Security Rule*;
    • HIPAA *Breach Notification Rule*
Protected Health Information

- **Protected Health Information** – is *ALL* information *held or transmitted* by the *pharmacy* or any of its business associates, in *ANY* form or media, whether *electronic, written, or oral* that:

1) Relates to an individual’s *past, present, or future physical or mental health or condition, for the provision of health care, or the past, present, or future payment for the provision of health care* to that individual, or

2) **Identifies the individual** or for which there is a *reasonable basis* to believe *such information* can be used to identify that individual (includes: name, address, birth date, social security number, employer, relatives, household members, plan ID, etc.)
Mandated ‘Uses & Disclosures’ of PHI

- PHI **MUST** be used and/or disclosed in only **TWO** situations:

  1) The *Individual* (or his/her *duly authorized* personal representatives) when the individual, subject to the PHI, *requests it*; or

  2) The *U.S. Dept. of Health and Human Services* requests it when they are undertaking a *compliance investigation, review or enforcement action*
Other ‘Uses & Disclosures” of PHI

- Additional to the two ‘mandatory disclosures’ PHI may be used and/or disclose in only **TWO** situations:

1) The ‘use or disclosure’ falls into one of the ‘Permitted Uses and Disclosures’ or,

2) The ‘use or disclosure’ falls within the ‘Authorized Uses and Disclosures’

3) “Any person making use of or disclosing PHI **MUST** make reasonable efforts to use, disclose, and request only the ‘minimum amount’ of protected PHI needed to accomplish the intended purpose.”
Other ‘Uses or Disclosures” of PHI

• Other uses and/or disclosers of PHI are allowed in only **TWO** situations:
  
1) The ‘use or disclosure’ falls into one of the ‘Permitted Uses and Disclosures’ or,

2) The ‘use or disclosure’ falls within the ‘Authorized Uses and Disclosures’
Permitted ‘Uses or Disclosures” of PHI

- **Permitted Uses and Disclosures of PHI:**
  1) To the *Individual* who is the *subject* of the *PHI*
  2) For the *Treatment, Payment, and Health Care Operations Activities;*

  ➢ *Treatment:* providing *health care services,* including *consultations* with *other providers* and *referrals* to other providers;

  ➢ *Payment:* includes *activities* of the pharmacy *to obtain reimbursement*;

  ➢ *Health Care Operations:* includes *quality assessment & improvement activities,* *medical or legal audits,* including *fraud and abuse detection and compliance programs,* *certain insurance functions,* and *administrative activities* by the pharmacy
Permitted ‘Uses or Disclosures” of PHI

Uses and Disclosures of PHI with Opportunity to Agree or Object:

1) Individual who is the subject of the PHI has informally given permission outright or, has clearly given the opportunity to ‘object’ and has not done so.

- Pharmacies may rely on the individual’s informal permission to disclose PHI to that individual’s family, relatives, or friends who are ‘directly involved’ in the individual’s health care or the payment of that health care.

- Example: A Pharmacy may dispense filled prescriptions to a person acting on behalf of the patient under Permitted Use and Disclosure.
Permitted ‘Uses or Disclosures’ of PHI

- **Incidental Uses and Disclosures of PHI:**

  - A *use or disclosure* of protected PHI is **Not** a violation of HIPAA if it is a *result of or incident to* an otherwise permitted use of disclosure.

  - Pharmacies should have a policy that ‘Incidental Uses and Disclosures’ of PHI are to be designed to safeguard ‘incidental use and disclosures’ and to limit them to the **absolute minimum information** necessary.

  - Example: *Leaving a message on a home voice mail.*
**Permitted ‘Uses or Disclosures” of PHI**

- **Uses and Disclosures of PHI Required By Law and for Similar Purposes: Protected PHI may be used or disclosed in the following situations related to compliance with the law and public health matters.**

1) Use and disclosure to public health authorities;
   
   a) entities regulated by the FDA for FDA-regulatory related information;
   
   b) Individuals who may have been exposed to a communicable disease when notification is authorized by law;
   
   c) Employers with respect to information concerning work-related illness or injury as required by OSHA, the Mine Safety and Health Administration, or state law;
Permitted ‘Uses or Disclosures” of PHI

- Use or Disclosure to Appropriate Government Authorities:

1) Use and disclosure to appropriate government authorities regarding victims of abuse, neglect, or domestic violence;

2) Use and Disclosure to Health Oversight Agencies for legally authorized activities such as:
   - Audits and investigations necessary for oversight of the health care system and government benefit programs (i.e. Medicaid/Medicare)

3) Use and disclosure in a judicial or administrative proceeding pursuant to an ‘order of the court or tribunal,’ a subpoena, or other lawful process.

4) Use and Disclosure to ‘law enforcement’ personnel for identifying or locating a suspect, fugitive, material witness, or missing person;
Permitted ‘Uses or Disclosures” of PHI

• Use or Disclosure to Appropriate Government Authorities:

1) Use and Disclosure to ‘law enforcement’ personnel in response to request for information about a victim or suspected victim of a crime;

- To alert law enforcement of a person’s death if criminal activity is believed to have caused it;
- When the protected health information is believed to be evidence of a crime occurring on premises; or
- In a medical emergency when necessary to inform law enforcement about a crime.
**Permitted ‘Uses or Disclosures” of PHI**

- Use or Disclosure to **Appropriate** Government Authorities:

  1) Use and Disclosure to *funeral directors, coroners and medical examiners, as needed, to determine the cause of death or to identify a deceased person*;

  2) Use or disclosure to *facilitate the donation and transplantation of cadaveric organs, eyes, and tissue*;

  3) Use or disclosure for *research purposes*, under certain **limited** circumstances;

  4) Use of disclosure that is believed to be necessary *to prevent or lessen a serious and imminent threat to a person or the public*;

  5) Use or disclosure for certain *essential governmental functions*, including military, intelligence, and national security functions, protective services for the President and eligibility for government benefit programs.
Authorized ‘Uses or Disclosures” of PHI

• **Limited Data Set Uses and Disclosures of PHI:**
  1) Research;
  2) Health care operations; and
  3) Public purposes

• **Provided that certain Specific Direct Identifiers are Redacted and Individual enters into a data use agreement:**
  1) Individual’s relatives;
  2) Household members;
  3) Employer;
  4) Plan ID #’s, etc.
Authorized ‘Uses or Disclosures” of PHI

• Limited Fundraising Uses and Disclosures of PHI:

1) Certain PHI can be used and disclosed to:

   a) A Business Associate; or

   b) Institutionally-related Foundation for the purpose of fundraising

   c) All proposed uses and disclosures used for fundraisers should be approved in advance by the Privacy Officer

➢ Any person seeking to use or disclose PHI for any purpose or in any situation not identified as a “Permitted Use and Disclosure” MUST obtain ‘written’ authorization of the individual who is the subject of the PHI. When in doubt, FILL IT OUT!
Distribution of Privacy Notices

• In your HIPAA Policies & Procedures, you need to explain the various ways that an individual’s PHI may be used and/or disclosed and explain to the individual their ‘rights’ concerning the privacy of his/her PHI.

• Alteration of your pharmacy’s standard Privacy Practices Notice can only be done by your Privacy Officer!

• Pharmacies should provide a copy of your standard Privacy Practices Notice to your patients not later than the first service encounter. If this is a face-to-face encounter, it must be given to the patient personally.

• If the first encounter is electronic, the Privacy Practices Notice should be provided contemporaneously via an electronic response.
Distribution of Privacy Notices

- If the first service encounter is by telephone, the Privacy Practice Notice must be given by a prompt mailing.

- Employees providing the Privacy Practices Notice must obtain a written acknowledgment of the patient that he/she has received the Privacy Practices Notice.

- Pharmacies’ HIPAA Privacy Practices Notice Policies & Procedures should instruct employees that if they fail to ensure the delivery of a Privacy Practices Notice on the first service encounter, that they are subject to being disciplined.

- Pharmacies must prominently display their Privacy Practices Notices on your web site and in the pharmacy where people seeking service may reasonably be expected to be able to read the notice. Notice should be at end of emails sent to patients.
Electronic Protected Health Information

- Pharmacies are responsible for establishing and maintaining appropriate safeguards to prevent unauthorized access to electronic protected health information.

- Pharmacies must periodically review and modify their security measures as needed to continue to provide reasonable and appropriate protection of e-PHI.

- Pharmacies must conduct an assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of e-PHI.

- Pharmacies must put in place security measures sufficient to reduce those risks and vulnerabilities.
e-PHI and the Privacy Officer

• The *Privacy Officer*, with appropriate IT personnel, should *regularly review* information records of *system activity*, including:
  – Audit logs;
  – access reports; and
  – Security incident reports

• The *Privacy Officer*, with appropriate IT personnel, should *ensure* that **ONLY** those *persons authorized to access to PHI* have the capability to do so. *No sharing access codes!*
e-PHI Security Measures

- **ALL** e-PHI should be stored on a *secure network*;
- Personnel able to access e-PHI should have a *“unique user identification number”* or *“complex passwords”*;
- Access to e-PHI should **ONLY** be *accessible to workstations* regularly used for access to e-PHI by *authorized personnel*;
- Privacy Officer should ensure that *access to e-PHI is terminated* for any individual *whose employment* with the pharmacy *ends or changes such that his/her duties no longer warrant such access*;
e-PHI Security Measures

- Privacy Officer must document all known or suspected security incidents, including attempted or successful unauthorized access, use, disclosure, modifications, or destruction of information or interference with information system’s operations.

- Privacy Officer must have a contingency plan for responding to emergencies, such as fire, vandalism, system failure or natural disaster, to maintain retrievable exact copies of e-PHI.
**e-PHI Security Measures**

- The pharmacy should implement *‘physical’ safeguards* to *limit access to e-PHI systems and facilities* in which they are housed;

- Areas where workstations having access to e-PHI should be in a *secure area accessed by electronic key codes*;

- Each *authorized employee* having access to these secure areas should have their own *electronic key code* with *entry into the secured area documented through an electronic logging of all key codes*;
e-PHI Security Measures

• Workstation areas should be designed to be hidden from view of patients and non-authorized personnel;

• e-PHI systems must have technical controls in place to prevent the ‘transferring’ of e-PHI from workstations to portable computer memory devices (i.e. thumb drives, CDs, etc.);

• Your pharmacy should have a policy on the ‘deleting’ of e-PHI and the re-use of electronic media that may have had e-PHI on it.
Inadvertent Disclosures of PHI

• The pharmacy should *mitigate to the fullest extent possible* any *harmful effects* that could flow from the *unauthorized disclosure of PHI*. All *unauthorized disclosures should be reported immediately to the Privacy Officer*. 
Notification of Breach of Unsecured PHI

• The Omnibus Rule (HITECH) replaces the current ‘significant risk of harm’ standard with a new ‘low probability of compromise’ standard.

• Security breaches involving 500 or more individuals **MUST** be reported to the Secretary of the U.S. Dept. of Health and Human Services ‘immediately’ (concurrently with notification to individuals)

• Security breaches involving **less than 500** individuals **MUST** be reported to the Secretary of U.S. Health and Human Services within **60 days following the end of the year in which the breach occurred.**
Notification of Breach of Unsecured PHI

- Upon *discovery of a breach* of unsecured PHI, the pharmacy *should notify each individual* whose unsecured PHI has been or is *reasonably believed* to have been accessed, acquired, used, or disclosed as a result of a breach;

- Such notification should be made as soon as reasonable practicable and in **NO** case *more than 60 days* after the breach is discovered. *If over 500 individuals*, notification to HHS and the individuals *must be immediate*. 


New Notification of Breach Standard

- Upon *discovery of a potential breach* of unsecured PHI, the *pharmacy* or *business associate* *MUST* provide a notice of breach of PHI ‘absent’ a finding that there was a ‘*low probability that the PHI has been compromised.*’

- *For example:* An *inappropriate mailing* of an *Explanation of Benefits* (“EOB”) consisting of data such as names, addresses, dates of services and amounts paid *would be a reportable breach,* ‘absent’ other mitigating circumstances.
  - *Example:* EOB’s were inadvertently mass mailed to the employer and they were either returned ‘unopened’ or ‘handed out’ to each employee unopened. This may be mitigating circumstances.
New Notification of Breach Standard

- The Omnibus Rule standard **REQUIRES** a **Risk Analysis** as to whether the *security incident will give rise to a disclosure to the Privacy Rule requirements*, including the minimum necessary standard.

- A *Covered Entity* or *Business Associate* can do a notification *without first doing* a risk analysis.

- Replaces the breach standard under the old Interim Final Rule from: *“Is there significant risk of harm?”* with the new Omnibus Rule standard question: *‘Is there a low probability of compromise?’*
Factors to Consider When Conducting a Risk Analysis for ‘Low Probability’

- Consider the ‘Nature and Extent’ of the PHI data involved, including ‘types of identifiers,’ as well as, likelihood of ‘re-identification.’

- In the past, ‘limited data sets’ that did not contain DOB’s and/or zip codes were not reportable but are now reportable under the new Omnibus Rule under the ‘low probability of compromise’ risk.

- Just determining that the ‘Risk of Harm’ is low does not remove this breach of a limited data set from a reportable to non-reportable category UNLESS the ‘Probability of Compromise’ is low.
Factors to Consider When Conducting a Risk Analysis for ‘Low Probability’

- The unauthorized individual’s *ability* (professional, legal, technical skills) that would either ‘restrict’ or ‘enhance’ their ability to ‘exploit’ (compromise) the PHI.

- *For example:* An employer receiving information containing ‘dates of health service’ and ‘diagnoses’ of certain employees (no names) would be ‘impermissible.’ Why?

- An employer may be able to *match those dates of service and diagnosis services* with *employee absentee records.*
Factors to Consider When Conducting a Risk Analysis for ‘Low Probability’

• You **MUST** establish that the PHI, once re-secured, was never actually copied, used, viewed or otherwise compromised.

• *For example:* Loss of a laptop computer containing PHI. The laptop was recovered and forensic analysis of the laptop showed that there was no breach of the data. Some laptops/PC’s come with facial recognition software that does not allow anyone else to access the laptop or PC.

• *Under this circumstance, the covered entity (pharmacy) or business associate may ‘reasonably’ determine that the information contained on the laptop was not compromised thereby, meeting the ‘low probability of compromise’ standard*
Factors to Consider When Conducting a Risk Analysis for ‘Low Probability’

- The Omnibus Rule provides **three exceptions** to a breach by a covered entity (pharmacy) or business associate that **allows them to conclude that no breach of PHI has occurred without having to conduct a risk analysis**:
  - When *unintentional access, use or disclosure of PHI* by a person acting under the authority of a covered entity and/or business associate (where access, use or disclosure) **was done in good faith and within the course of the scope of the relationship**;
  - The *inadvertent disclosure*’ was made by one person *‘authorized’* to have access to another *‘unauthorized’* person within the same facility; and
Factors to Consider When Conducting a Risk Analysis for ‘Low Probability’

- The unintentional access, use or disclosure of PHI to an ‘unauthorized’ person where the person cannot reasonably retain the information.
- **For example:** Hospital setting in a non-private room
- By definition, encrypted PHI, using an approved methodology cannot be accessed, used or disclosed (*assuming the encryption ‘key’ has not been otherwise compromised*).
- **Caution:** Software and Hardware encryption standards ‘change’ all the time. Make sure you are making required updates.
New Restrictions on Using PHI for Marketing Purposes

- The Omnibus Rule *significantly expands* the definition of ‘marketing’ to include previously ‘excluded’ communications that now require ‘prior written permission.’
- Previously under the Privacy Rule, ‘marketing’ communications relating to treatment, health care operations, as well as, certain other activities, such as care coordination were ‘excluded.’
- The Omnibus Rule limits ‘excluded’ marketing communications to only those that were NOT made in exchange for payments either directly or indirectly from a Third Party. (‘Subsidized’ communications) They now ‘require prior written permission’ (This includes mailing houses, excludes ‘in-kind’ marketing materials or communications for a treatment or care coordination program such as refill reminders)
New Restrictions on Using PHI for Marketing Purposes

• Practical Tips for Marketing Communications:
  • Does the communication involve the use or disclosure of PHI?
  • Is the communication intended to encourage an individual to purchase or use a product or service (as opposed to a communication intended to inform individuals about the implementation of a new product or service)?
  • Will inducements from a Third Party be a financial payment or an in-kind payment?
New Potential Increases in Liability for Covered Entities for Acts of Business Associates

- Under the Privacy Rule, Acts or Omissions of Covered Entities’ Business Associates ‘acting’ as an ‘agent’ for the covered did not create a liability for the Covered Entity if the covered entity:
  - Complied with administrative safeguards, as well as, used ‘disclosure’ requirements with respect to their business associates, and
  - Did not know of the pattern or practice of the business associate at issue and who failed to act as required by the Privacy Rule.
- NEW: Omnibus Rule: ‘Removes’ this exception making covered entities ‘liable’ for acts of their business associates even where the covered entity complied with its contractual obligations and had no knowledge of the wrongdoing.
Business Associate Threshold as an ‘Agent’ of a Covered Entity

• Under the Omnibus Rule, terms, statements or labels given to Third Parties (e.g. independent contractor) DO NOT control whether and ‘agency’ relationship exists.

• Instead, it’s the manner and method in which a covered entity actually controls the service provided that decides the ‘agent’ designation which includes:
  – Time, place and purpose of a business associate’s conduct;
  – Did the business associate engage in a course of conduct subject to a covered entity’s control?
  – Was the conduct by the business associate commonly done by a business associate to accomplish the service performed on behalf of a covered entity?
  – Could the covered entity reasonably expect that a business associate would engage in the conduct in question?
**PHI Breaches by a Business Associate ‘Agent’ of a for a Covered Entity**

- **Breach Notification Timing:** If a Business Associate is acting *as an ‘agent’ for a covered entity*, then when the business associate *discovers* a breach, it is *attributed to the Covered Entity*, then
  - The Covered Entity **MUST** *provide notifications* based on the *time* the business associate *discovers* the breach **NOT** from the time the business associate *notifies* the covered entity.
Direct Liability of Business Associates

- The Omnibus Rule is very clear as it relates to a ‘direct’ liability of a business associate when:
  - The business associate uses and discloses PHI in violation of its business associate agreement or the Privacy Rule;
  - Fails to disclose PHI when an individual or the Secretary of HHS requests:
    - Fails to make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request; and
    - Fails to enter into a business associate agreement with ‘subcontractors’ who create, receive, maintain, or transmit PHI on behalf of a ‘business associate.’
Direct Liability of Business Associates

- Business Associates **MUST** implement *appropriate security measures* to protect ‘*electronic PHI*’ including performing ‘*risk analysis*’ to identify *vulnerabilities to the confidentiality, integrity and security of electronic PHI*.
Compliance by Covered Entities and Business Associates

- The Omnibus Rule provides that those business associates already operating under a business associate agreement are granted a grace period to modify existing agreements.

- Covered entities and business associates will be deemed in compliance with the new standard if:
  - 1.) prior to January 25, 2013, the entities have entered into and are operating under a business associate agreement that has met the requirements of the Privacy Rule that were in effect on that date; and
  - 2.) the contract or arrangement is not modified or renewed from March 26, 2013 to September 23, 2013.
Policy of Non-Intimidation/Non-Retaliation

• Pharmacies should have a policy of non-intimidation – non-retaliation against any employee, officer or director, or any patient, for compliance with the pharmacy’s Policy or HIPAA requirements, or for exercising or attempting to exercise his/her rights under HIPAA. This includes:

  ➢ Refusing to authorize a disclosure;
  ➢ Filing a complaint;
  ➢ Requesting a disclosure accounting;
  ➢ Participating in an investigation; or
  ➢ Opposing an inappropriate practice
Document and Record Retention

- Pharmacies should maintain all privacy policies, procedures, privacy practices notices, complaints, dispositions of complaints, written communications, written authorizations, and other documents related to Policy or HIPAA for a minimum of 6 years…
Post HIPAA CE Exam

1.) Which laws below govern confidentiality?
   - B.) The Medicare Act
   - C.) HIPAA
   - D.) All of the above
Post HIPAA CE Exam

2.) The recent updates to privacy laws is known under what name?
   - A.) The Privacy Rule
   - B.) HITECH or Omnibus Rule
   - C.) HIPAA Act of 1996
   - D.) None of the above
3.) What are the monetary penalties under HIPAA and HITECH rules for ‘willful neglect’
   - A.) $100 per violation or $25,000 per year
   - B.) A ‘maximum’ of $50,000 per violation or $1.5 mil. Per year
   - C.) A ‘minimum’ of $50,000 per violation and no maximum amount
   - D.) $25,000 per violation, no maximum.
Post HIPAA CE Exam

4.) Your HIPAA Policies & Procedures MUST include which element(s)?
   - A.) Detailed guidelines as to ‘what’ patient information is ‘added’ to patient records
   - B.) Instructions as to the ‘length of time’ these records are to be maintained
   - C.) Step by step instructions on ‘how’ these records are to be disposed of and destroyed
   - D.) All of the above
Post HIPAA CE Exam

• 5.) Which of the following **IS NOT** a part of the required HIPAA training as it relates to staff?
  - A.) HIPAA Privacy Rule
  - B.) HIPAA Security Rule
  - C.) HIPAA Breach Notification Rule
  - D.) HIPAA Associate Agreements
Post HIPAA CE Exam

6.) Which two circumstances require ‘mandated’ use and/or disclosure of Personal Health Information (PHI)?
   - A.) Individual requests and US HHS request
   - B.) Individual requests and for treatment, payment and Health Care operations
   - C.) Treatment, payment, Health Care operations and audits
   - D.) Law enforcement and administrative proceedings
• 7.) Which of the following are ‘permitted uses’ of PHI?
  – A.) appropriate government authorities investigating victims of abuse, neglect, or domestic violence
  – B.) Individuals who may have been exposed to a communicable disease
  – C.) Pursuant to a court order or subpoena
  – D.) All of the above
Post HIPAA CE Exam

• 8.) Which of the following is NOT a ‘authorized use’ of PHI?
  – A.) Public Purposes
  – B.) Research
  – C.) Employer hiring
  – D.) Health Care operations
Post HIPAA CE Exam

9.) As it relates to the distribution of Privacy Notices, which of the following is false?

- A.) You must provide a prompt mailing of the Privacy Notice if the first service encounter is by phone
- B.) Employees must obtain written acknowledgement from the patient that he/she has received the Privacy Notice
- C.) Privacy notices MUST be prominently displayed in the pharmacy but DO NOT have to be displayed on your web site.
- D.) Your HIPAA Policies & Procedures should instruct employees that they are subject to discipline if they fail to provide a Privacy Notice on the first service encounter.
Post HIPAA CE Exam

• 10.) The Privacy Officer, along with the appropriate IT personnel should regularly review which of the following?
   – A.) HIPAA Audit logs
   – B.) Access Reports
   – C.) Security Incident Reports
   – D.) All of the above
Post HIPAA CE Exam

• 11.) Notification of Breach of Unsecured PHI of 500 individuals or more must?
  – A.) Be reported to the Secretary of HHS within 60 days within days of the security breach
  – B.) Be reported to the Secretary of HHS immediately
  – C.) Be reported 60 days following the end of the year in which the breach occurred.
  – D.) Be reported within 60 days of notifying the individuals of the PHI security breach.
• 12.) Under the new Omnibus Rule (HITECH), the discovery of a potential breach of unsecured PHI, the pharmacy or business associate **MUST** provide? (best answer)
  
  – A.) Notice of the breach ‘absent’ a finding that there was a ‘low probability that the PHI has been compromised’
  
  – B.) No notice of a breach if under 500 individuals
  
  – C.) A notice of breach to the Secretary of HHS only
  
  – D.) Notice of breach regardless of a finding of a ‘low probability that the PHI has been compromised.’
Post HIPAA CE Exam

13.) Which of the following IS NOT an ‘exception’ to a breach by which a covered entity or business associate is allowed to conclude that no breach of PHI occurred?

- A.) The employee certifies that they did not use or release any unsecured PHI
- B.) When the unintentional access, use or disclosure of PHI was done in good faith and within the course of the scope of the relationship
- C.) When access, use or disclosure of PHI was ‘inadvertent’ and was made by a person who is ‘authorized’ to an ‘unauthorized’ person within the same facility
- D.) The unintentional access, use or disclosure of PHI to an unauthorized person where the person cannot be reasonably expected to retain the information.
Post HIPAA CE Exam

• 14.) The new Omnibus Rule limits ‘excluded’ marketing communications to only those that?
  – A.) Were not made in exchange for payments either directly or indirectly from a Third Party
  – B.) Involve the use or disclosure of PHI
  – C.) Encourage the individual to purchase a product or service
  – D.) None of the above
Post HIPAA CE Exam

15.) Under the new Omnibus Rule, covered entities are now liable for acts of their business associates?
   - A.) Under no circumstances
   - B.) Only in cases were the business associate failed to report to the HIPAA violation to the covered entity
   - C.) Even where the covered entity complied with its contractual obligations and had no knowledge of the wrongdoing
   - D.) Only in cases where the business associate is an independent contractor.