BSM Connection®
Distance Learning

A Guide to HIPAA (Health Insurance Portability and Accountability Act) and Patient Confidentiality
# Table of Contents

- **OVERVIEW** ......................................................................................................................... 1  
- **HIPAA: A BRIEF CHRONOLOGY** ...................................................................................... 1  
- **MOST RECENT HIPAA ADDITION: THE FINAL RULE** ..................................................... 1  
- **WHO IS COVERED BY HIPAA?** ........................................................................................ 2  
- **HIPAA ELEMENTS AND REQUIREMENTS** ....................................................................... 2  
- **PRIVACY RULE** .................................................................................................................. 3  
- **SECURITY RULE** ................................................................................................................ 6  
- **BREACH NOTIFICATION RULE** ....................................................................................... 9  
- **RESPONSIBILITIES OF INDIVIDUALS** ............................................................................. 11  
- **CONCLUSION** .................................................................................................................... 12  
- **COURSE EXAMINATION** .................................................................................................... 13
OVERVIEW

The goal of providing increased protection for confidential health care information began when Congress enacted the 1996 Health Insurance Portability and Accountability Act, or HIPAA. This act developed from early health-care reform efforts and resulted in significant changes to the way confidential health care was managed by providers. Since then, subsequent directives expressed under the primary umbrella of HIPAA have emerged to improve and strengthen privacy protection while accommodating new business and technological needs. As one might guess, all of these directives resulted in continued changes to how providers and associates conduct daily operational tasks.

Although a complex act, HIPAA and all related federal directives share a primary purpose: to protect the privacy, integrity and availability of protected health information or PHI, whenever the patient receives services provided by health facilities, physicians, and health plans. This course provides an overview of all HIPAA elements and examines current regulatory and compliance directives falling under the auspices of the HIPAA privacy and security rules. These include requirements established by the most recent 2013 HIPAA Omnibus Final Rule. With this knowledge, providers and associates will be able to conduct daily operational tasks in a manner that upholds HIPAA laws and provides maximum security of confidential health care information.

Note: Health care entities may use this course to provide the required HIPAA training for any person with access to personal and confidential health information protected by these mandates.

HIPAA: A BRIEF CHRONOLOGY

<table>
<thead>
<tr>
<th>HIPAA enacted</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Security Rule for Protected Health Information (PHI)</td>
<td>1996</td>
</tr>
<tr>
<td>Health Information Technology for Economic and Clinical Act (HITECH) (Facilitates the adoption of electronic records and strengthens breach notification requirements.)</td>
<td>2002</td>
</tr>
<tr>
<td>American Recovery and Reinvestment Act (ARRA)</td>
<td>2009</td>
</tr>
<tr>
<td>HIPAA Omnibus Final Rule (Broadens the scope of privacy and security of business associates and their subcontractors; increases patient accessibility to and control over medical records.)</td>
<td>2013</td>
</tr>
</tbody>
</table>

MOST RECENT HIPAA ADDITION: THE FINAL RULE

The Omnibus Final Rule, known informally as the Final Rule, is the most recent legislation affecting HIPAA regulation and compliance. Published in January 2013 by the Department of Health and Human Services (HHS), the Final Rule serves to strengthen the protection and security of confidential health information through substantial changes to existing HIPAA and HITECH requirements. These changes are summarized in the following paragraphs, and are captured in both the Privacy Rule and Security Rule sections later in the course.

A particularly important aspect of the 2013 legislation involves a renewed emphasis on privacy and security of PHI in relation to non-practice entities (called Business Associates or BA) working within the continuum of health care management. The Final Rule also expanded breach notification requirements of the HITECH Act, and establishes more significant penalties for breaches. Another key aspect of the Final Rule is its expansion of individual rights in relation to access and control of personal health care records. For example, patients now can ask for a copy of their medical record in an electronic format (from practices that support electronic medical records). Additionally, when a patient pays cash for a procedure, the patient can instruct the physician/provider not to share information about the treatment with his or her health plan (often called the "concealment rule").
WHO IS COVERED BY HIPAA?

Organizations that must comply with HIPAA guidelines include any health care provider who collects and transmits health care information. A “covered entity” includes any individual or organization with access to personal confidential health information. More specifically, a covered entity may be:

- Health care providers (medical practices/hospitals/pharmacies).
- Health care clearinghouses
- Health plans (insurers)

Business associates are vendors and their subcontractors who have a need to transmit, view, store or manage PHI in order to fulfill the services it is providing to the covered entity.

Training and Compliance

Because of the importance of HIPAA, health care entities are required to train all new staff and provide a refresher on HIPAA law to all employees annually. Documentation of this training should be complete and accurate in case of potential audits. Compliance with all HIPAA components is governed through the Office of Civil Rights (OCR), and violations of HIPAA requirements can result in serious financial and/or criminal consequences.

HIPAA ELEMENTS AND REQUIREMENTS

There are four main elements of HIPAA regulation: The Privacy Rule, the Security Rule, Insurance Portability, and Administrative Simplification (see table).

| REQUIREMENTS: |
| HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) |
| Privacy Rule: Requires the development of standards and regulations to protect the privacy of confidential health information while allowing information to flow between parties in order to promote high-quality health care and to protect the wellbeing of the general public. |
Security Rule: Establishes a national set of security standards for protecting health information that is transmitted or stored electronically.

Insurance Portability: Provides protection from losing insurance when employees change jobs or have pre-existing health conditions.

Administrative Simplification: Includes provisions in the HIPAA law requiring the Department of Health and Human Services (HHS) to implement national standards for electronic health care transactions.

As previously mentioned, this course focuses on privacy and security, the cornerstone of HIPAA policy. These rules require health care entities to develop and implement processes that safeguard patient confidentiality to the highest degree and include administrative, physical, and technical safeguards for ensuring that medical information is created, stored, transmitted, and received in a safe manner.

PRIVACY RULE

The major goal of the Privacy Rule is to define and protect an individual’s PHI while communicating/sharing information necessary to provide appropriate and timely medical care to patients. Most certainly, this can be a “balancing act”; however, proper protocols in handling confidential medical information are crucial to HIPAA compliance.

The HIPAA Privacy Rule requires that covered entities follow national standards regarding privacy of health information. In addition, Privacy Rule regulations provide patients certain rights in relation to accessing their health information, including the ability to examine and obtain copies of their health records and to request corrections.

Protected Health Information (PHI)

Further discussion of HIPAA privacy mandates a thorough understanding of a term presented earlier in the course: protected health information, or PHI. A definition of PHI is provided within the context of a summary of the Privacy Rule published by the HHS and OCR and reads as follows:

- The Privacy Rule protects all "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 Privacy Rule calls this information Protected Health Information (PHI). Extracted from the HHS/OCR Privacy Rule Summary.

PHI includes personal demographics or health information that is:

- Created by health care organizations.
- Received by health care organizations from patients, other providers, or health plans.
- Written.
- Spoken.
- Electronically transmitted.

<table>
<thead>
<tr>
<th>EXAMPLES OF PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name, address, social security number</td>
</tr>
<tr>
<td>Insurance eligibility and coverage information</td>
</tr>
<tr>
<td>Billing records, claims data, authorizations</td>
</tr>
<tr>
<td>Genetic information</td>
</tr>
<tr>
<td>Medical records (i.e., diagnosis, treatment, photos, x-rays, tests)</td>
</tr>
<tr>
<td>Research records</td>
</tr>
</tbody>
</table>
A Guide to HIPAA and Patient Confidentiality

PHI does **NOT** include:

- Employment records.
- Worker’s compensation information.
- Occupational Safety and Health Administration (OSHA) information.

![Records](image)

**Figure 3: Protected Health Information (PHI) includes all medical records, both paper and electronic.**

Permitted Uses and Disclosures of PHI

Written authorization for use and disclosure of PHI is required to protect patients from inappropriate disclosure to individuals or organizations. Examples include requests for information from an attorney without a subpoena and requests for information from creditors of patients. There are, however, many instances in which PHI may be disclosed without written authorization from an individual. PHI disclosures do not require a written authorization from a patient when involving:

1. **Treatment (coordination of care).** This includes the providing, coordinating, and managing of a patient’s health care by one or more health care providers. (Note: HITECH guidelines make it possible for entities nationwide to exchange electronic health records for the purpose of coordinating care.)

2. **Payment issues.** This includes obtaining payment or reimbursement for services provided by the “covered entity.”

3. **Health care operations.** This includes training, accrediting, certifying, credentialing, licensing, and evaluating the operational performance of a practice.

4. **Requests from individuals for their own health care records.** Patients may request an electronic copy of their medical record. If the practices do not have EHR or this capability, then a paper version may be provided.

5. **Audits by certain governmental agencies.** These include audits by HHS and OCR.

6. **Law enforcement.** For example, information needed in cases of abuse and neglect.

“Incidental disclosure” of PHI is a situation where the use or disclosure of PHI cannot reasonably be prevented. It is usually limited in nature and occurs “incidentally” as a result of a permitted disclosure. Examples of incidental disclosures include:

- Hearing a patient’s name called out loud for escort from one area to another.
- Overhearing a physician phone conversation regarding another patient.
- Seeing information on a whiteboard in a medical facility.
“Minimum necessary disclosure” of PHI requires that a “covered entity” make every effort to request and/or disclose only the minimal amount of information necessary for a specific purpose. Covered entities must establish policies and procedures to ensure minimum disclosure. Exceptions to the minimal necessary guidelines are allowed when disclosure is made to medical providers for treatment, to individuals for their own health care records, to HHS/OCR for enforcement, or to law enforcement personnel. The HIPAA Privacy Rule applies to the PHI of a decedent for 50 years following the date of death of the individual.

**Notice of Privacy Practices (NPP)**

Under its Privacy Rule, HIPAA requires covered entities to develop and provide a Notice of Privacy Practices (NPP) for individuals accessing services. Patient acknowledgement of the receipt of the NPP is optimal; however, if an individual declines signing an acknowledgment, documentation should be made of the declination.

The following table describes elements that must be included in the NPP. In regards to notifying patients of NPP updates that include the elements required for compliance, practices are required only to make the notice available to patients as they visit the office. (It is not necessary for a practice to attempt to “catch up” with prior patients to notify them of the changes.)

HELPFUL HINT: Practices should consider daily operational routines when updating their NPP so that any pertinent material can be included. For example, offices that use sign-in sheets and/or call patients' names aloud in the waiting room should clearly communicate in the NPP that those practices will occur. As long as patients have been notified and they agree (by signing the notice), the risk of violating privacy becomes a nonissue.

**Figure 4:** All patients visiting the office must receive an updated Notice of Privacy Practices (NPP) that includes changes as indicated in the Final Rule of 2013. It is preferred that patients sign an acknowledgment of receipt, but it is not required.
REQUIRED ELEMENTS: NOTICE OF PRIVACY PRACTICES (NPP)

| Description of the individual’s right to restrict certain disclosures of PHI to a health plan when the individual pays out of pocket and in full for the health care item or service (Required addition to NPP as indicated by the 2013 Final Rule) |
| Designation of a contact person (usually the privacy officer) for individuals needing assistance regarding privacy issues |
| Rights of individuals regarding their PHI |
| • Method to access information |
| • Ability to amend PHI if inaccurate or incomplete |
| • Accounting of disclosure of PHI to other individuals (excluding incidental disclosure) |
| • Option to request restrictions as to PHI use (the entity is under no obligation to comply) |
| • Option to request specific methods of communication of PHI (e.g., specific phone number, no post cards, etc.) |
| Permission to release psychotherapy notes |
| Permission to use PHI for marketing purposes |
| Description of the patient’s right to opt out of fundraising |
| Description of the patient’s right to be notified in the event of a breach |
| Protocols that require a copy of the NPP be provided to all individuals who access services of the covered entity |
| Request for acknowledgement of receipt of the NPP (not required) |

Note: Each covered entity is required to have a privacy officer who establishes and implements the above elements.

SECURITY RULE

The Security Rule is a component of HIPAA/HITECH Act that requires covered entities to maintain administrative, physical, and technical safeguards to prevent either intentional or unintentional improper disclosure of electronic PHI. The rule states that covered entities are responsible for ensuring the confidentiality, integrity, and availability of PHI that has been created, received, maintained, or transmitted to others, specifically PHI shared with what the rule refers to as a business associate and/or a subcontractor of the business associate. It further mandates that the covered entity is responsible for reasonably anticipating any potential threats and hazards that would compromise confidentiality.

Business Associates and Subcontractors

Business associates and any/all subcontractors of the business associate must comply with all applicable requirements set forth by HIPAA. In brief, this means covered entities are required to enter into HIPAA-compliant contracts with their business associates who must do likewise with their subcontractors, who must do likewise with theirs, and so on. While the following definitions offer cursory descriptions of a business associate and a subcontractor, it is prudent for practices to review the HHS definitions very carefully. The practice should revise and update business associate agreements to include the all requirements of the business associate’s subcontractor(s).

• Business associate. For HIPAA’s purposes, a business associate. This includes “one who creates, maintains, or transmits PHI on behalf of a covered entity for a function or activity that is regulated under HIPAA.” HITECH dictates that anyone involved in data transmission services of PHI for covered entities (and their business associates) must be treated as a business associate. Examples of business associates include, but are not limited to: e-prescribing gateways and other companies that provide data transmission services to covered entities with respect to PHI and Security Rule requirements. Additionally, any company that provides data storage and other maintenance services requiring ongoing access to PHI is clearly considered a business associate and therefore must comply with HIPAA’s privacy and security standards during the normal conduct of their business with the covered entity.

• Subcontractor. In 2013, the Department of Health and Human Services (HHS) implemented an expanded definition of a subcontractor that includes any person to whom a business associate
delegates a function, activity, or service other than in the capacity of the business associate’s workforce. Because of this change, a subcontractor of the business associate must comply with HIPAA privacy and security rules. The subcontractor is also subject to the same audits and penalties for noncompliance for which the business associate and the covered entity are liable should a PHI breach occur. These same rules continue downstream and extend to subcontractors of subcontractors. Such contracts should be managed very carefully to comply with multiple levels of restrictions.

Administrative Safeguards

Administrative safeguards used to protect patient confidentiality include:

- Designating a **privacy officer** to develop and implement security policies.
- Considering the addition of cyber insurance as an added layer of protection for the practice.
- Requiring agreements from business associates (lawyers, consultants, auditors, billing companies, pharmacists, etc.) that stipulate protocols and procedures to protect PHI.
- Placing increased emphasis on subcontractors of business associates. For example, when a relationship exists, a subcontractor of a business associate is required to sign a HIPAA-compliant business associate agreement. Additionally, subcontractors of subcontractors who have access to PHI through the services they provide must also enter into a HIPAA-compliant business associate agreement. Examples include e-prescribing gateways and other subcontractors downstream in processing electronic health care information.
- Conducting a risk analysis (recommended at least annually) of the covered entity and implementing corrective actions identified through the risk analysis.
- Initiating an information system activity review and developing contingency plans in case of a breach.
- Conducting training for all employees on HIPAA policies, guidelines, and consequences of a breach of PHI policy.
- Establishing procedures to prevent terminated employees from accessing any confidential information after termination.

Figure 5: Shredding documents that contain private information is one way of ensuring HIPAA compliance.
Monitoring and protecting information on electronic devices is suggested to ensure that all PHI is encrypted. Mobile devices such as smart phones, tablets and laptops must be monitored carefully to protect ePHI.

Physical Safeguards

Physical safeguards used to protect patient confidentiality include:

- Establishing guidelines for workstation use and security.
- Establishing device and media controls in the handling of electronic information. These include precautions to protect systems and equipment, which may include surge protectors, back-up systems, etc.)
- Shredding documents properly and according to protocols.
- Developing and implementing policies and protocols for the use of all electronic devices containing protected health information. These protocols must provide guidelines for desktop computers and practice-owned mobile devices such as laptops, tablets, and smartphones and should include the utilization of a system that can perform remote wiping/cleaning if any device is lost or stolen.
- Locating computer monitors in locations that limit unintentional disclosure of PHI.
- Maintaining storage of PHI in a secure area.
- Clearing, purging, or destroying PHI on electronic media by an IT professional.

![Figure 6: Health care entities must develop protocols that include appropriate use of smartphones and other mobile electronic devices that contain private information.](image)

Technical Safeguards

Technical safeguards used to protect patient confidentiality include:

- Using unique names and/or numbers to identify and track user information. You should have policies governing issues such as password complexity with intervals of regular password change. Symbols and upper and lowercase letters must be combined in passwords or logins. Practices must also define procedures for accessing electronic information in case of emergencies.
• Installing and updating antivirus software and firewalls.

• Developing audit controls to track the activity of hardware and software use.

• Using encryption to maintain the security of electronically transmitted PHI.

• Initiating an annual IT system risk analysis and certification by a qualified person (and maintaining appropriate records indicating certification and testing) to make certain that the system is safe from intrusion by hackers or other unauthorized sources.

Figure 7: Unique login and password systems are considered technical safeguards.

**BREACH NOTIFICATION RULE**

While HIPAA has always required notification of breaches to internal governance (the privacy officer), there has been a recent expansion of notification requirements as directed by the Final Rule. The HITECH Act makes specific provisions to ensure accountability of health care entities for the proper safeguarding of protected health information.

The HITECH Act adds emphasis to the privacy requirements outlined in HIPAA and adds additional notification requirements in the event of a breach of confidential information. Severe penalties, including civil, criminal, and financial, may result when breaches occur. The Final Rule of 2013 increases the stakes whenever a practice experiences a data breach. If a breach is suspected, the responsibility falls to the covered entity/practice to prove that a data breach did **NOT** compromise PHI.

**Breach Risk Assessment**

In order to determine whether a breach notification is indicated, the responsible practice should immediately refer to the updated HIPAA guidelines (as written in the 2013 Final Rule) and carefully perform a thorough risk assessment, including the following tasks:

• **Gather and review information when an incident is reported to determine the nature and extent of PHI disclosed.** If the information released contained social security numbers, credit card numbers, or other personally identifiable information, it would be considered a significant breach of PHI.

• **Assess and determine to whom the PHI was disclosed or received.** Review the risk and capability of the person to use the information to access additional protected information that would enable him or her to identify the patient.

• **Determine whether the PHI was actually acquired or reviewed and to whom.** For example, if a missing smartphone, mobile device, or any other electronic device containing PHI is recovered,
the practice may need to perform a careful analysis in order to determine the likelihood of the data truly being used or stolen. Practices should develop a strict policy to remotely “wipe clean” any mobile electronic devices/smartphones/tablets, etc. in the event that such a device is lost or stolen.

- **Determine the extent to which the risk to the information has been mitigated.** Attempt to follow up and to show that assurances were received from the recipient that the information accessed will not be disclosed.

- **Establish clear time frames of the information released.**

Assigning the assessment task to an experienced manager is critical, as tasks and information MUST be carefully and accurately documented. Managers must record dates, times, and all pertinent information during the investigation process. Employees involved in the assessment process—as well as any interviews and processes utilized—also should be documented.

**Managing a Breach**

When a breach is identified, practices should first refer to an updated HIPAA breach policy that reflects all 2013 changes. When applicable, managers can use these guidelines (with the data collected during the risk assessment) to substantiate that PHI was not jeopardized. The final step in handling a breach is conducting the formal notification of three entities.

The following outlines the details of these required notifications:

- **Affected individuals** must be notified by the covered entity if PHI has been improperly disclosed to entities not covered by privacy protocols and procedures required in the Privacy Rule.

- **HHS** must be notified annually of any instances in which the breach affected fewer than 500 individuals throughout the year.

- **HHS AND media outlets** must be notified if the breach affects 500 or more individuals.

Each individual with access to PHI is responsible for following the protocols and guidelines established by the covered entity to protect the privacy of information **AND** for notifying the privacy officer should a breach occur.
**RESPONSIBILITIES OF INDIVIDUALS**

Each staff member of a covered entity has great personal responsibility in ensuring the confidentiality of PHI. Paying close attention to the policies and procedures developed by employers can greatly decrease the possibility of the unintentional disclosure of this information. Examples of ways individuals can support the confidentiality and privacy of health information are discussed in the accompanying table.

<table>
<thead>
<tr>
<th>INDIVIDUALS CAN …</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remember to use PHI only if it is necessary to perform specific duties.</td>
</tr>
<tr>
<td>Be discreet with PHI to avoid incidental disclosure as much as possible.</td>
</tr>
<tr>
<td>• Require staff to log off the computer when leaving a work station for any reason, no matter how brief.</td>
</tr>
<tr>
<td>• Speak softly and keep verbal exchanges to a minimum and away from patients.</td>
</tr>
<tr>
<td>• Limit personal discussions that might be overheard by patients or others.</td>
</tr>
<tr>
<td>• Keep written PHI in a secure location not visible to patients.</td>
</tr>
<tr>
<td>Practice “safe” computing.</td>
</tr>
<tr>
<td>• Choose a password that is complex and not easy to guess. Keep this information confidential and change as often as required by facility protocols. Never share or write down passwords.</td>
</tr>
<tr>
<td>• Log out of the computer when leaving a work station for any reason.</td>
</tr>
<tr>
<td>• Refrain from opening, forwarding, or replying to suspicious emails.</td>
</tr>
<tr>
<td>• Use email ONLY as protocols permit.</td>
</tr>
<tr>
<td>• Limit Internet access by staff to an as-needed basis as email usage provides opportunities for hackers and unauthorized access. Consider using software to limit Internet access by employees who do not need the Internet for job functions.</td>
</tr>
<tr>
<td>• Never install personal software on a facility computer without the written permission of the privacy/security officer.</td>
</tr>
<tr>
<td>Immediately report the following incidents to the privacy/security officer:</td>
</tr>
<tr>
<td>• Loss of any device containing PHI (e.g., tablet, laptop, smartphone).</td>
</tr>
<tr>
<td>• Any suspected threat to computer systems or PHI.</td>
</tr>
<tr>
<td>• Any suspected breaches of privacy.</td>
</tr>
<tr>
<td>• Loss of paperwork containing PHI.</td>
</tr>
<tr>
<td>Follow all policies and procedures as established by the employer to protect the privacy and confidentiality of health care information.</td>
</tr>
</tbody>
</table>

*Figure 8: Health care providers need to instruct staff how to protect a patient’s private information while using computers.*
CONCLUSION

As this course indicates, HIPAA and all related federal directives regarding PHI have drastically changed the manner in which health care entities function in their approach to protecting patient and practice confidentiality. Considering the HITECH additions made in 2009 and the release of the 2013 Final Rule, it is clear that policymakers are continuing to strengthen these protections to meet the changing needs of individuals and health care entities alike.

Learners should now have a clear understanding of HIPAA and all provisions relative to privacy and confidentiality including regulatory directives. With this information, health care personnel can put forth their best effort in complying with up-to-date HIPAA policies in an effort to maximize protection of the privacy and confidentiality of all individuals. It is the responsibility of each individual with access to PHI to be diligent in following procedures and protocols mandated by HIPAA/HITECH law to accomplish this goal.
COURSE EXAMINATION

1. HIPAA stands for:
   a. Health Information Portability and Accountability Act.
   d. Home Information Protection and Accountability Act.

2. One primary change included in the HIPAA Omnibus Final Rule of 2013 requires a business associate of the covered entity (physician practice) to sign a Business Associate Agreement with:
   a. Subcontractors of professional associations.
   b. Subcontractors of business associates.
   c. Subcontractors of optometrists.
   d. Subcontractors of affiliated hospitals.

3. According to regulations contained in the Omnibus Final Rule of 2013, a patient has the right to receive a copy of his or her medical record in an electronic format if the associated provider utilizes electronic health records.
   a. True
   b. False

4. Covered entities under HIPAA include:
   a. Lawyers.
   b. Health care providers.
   c. Health care facilities.
   d. Librarians.
   e. a and d.
   f. b and c.

5. Protected Health Information (PHI) includes:
   a. Demographic information on individuals.
   b. Insurance eligibility and coverage information.
   c. Billing records, claims data, referral authorizations.
   d. Medical records, diagnosis, genetic information, and testing.
   e. c and d.
   f. All of the above.

6. Entities covered under HIPAA are required to develop a Notice of Privacy Practices (NPP) and must make these available to individuals accessing services through the entity.
   a. True
   b. False

7. Which of the following disclosures require signed permission from the individual whose PHI is being requested?
   a. Referrals to physicians
   b. Consultations between physicians treating individuals
   c. Information requested by an attorney without a subpoena
   d. Information requested by insurance companies for payment purposes
8. Patient names on a sign-in form are considered an intentional breach of PHI.
   a. True
   b. False

9. Under the HITECH Act, the Breach Notification Act does NOT require notification to HHS of the intentional or unintentional disclosure of PHI to unapproved entities on an annual basis unless the breach has affected more than 500 individuals.
   a. True
   b. False

10. Notice of Privacy Practices (NPP) must be updated in 2013 to include which of the following?
    a. Names of the owners of the covered entity
    b. Names of companies that have access to PHI
    c. Patient’s right to restrict disclosures of PHI to a health plan when the patient pays out of pocket and in full for the health care item or service.
    d. Profitability of the covered entity

11. If an individual or staff member has a complaint regarding the use of PHI, the individual must speak with the facility’s:
    a. Manager.
    b. Owner.
    c. Maintenance coordinator.
    d. Privacy officer.
    e. Chief physician.

12. Which of the following is NOT an administrative safeguard requirement?
    a. Designating a privacy officer
    b. Developing a cost analysis of HIPAA requirements
    c. Obtaining HIPAA-compliant business associate agreements for subcontractors
    d. Establishing procedures to prevent terminated employees from obtaining access to confidential information after termination

13. Physical safeguards do NOT include which of the following?
    a. Posting PHI on a white board in the facility
    b. Storage of PHI in a secure place
    c. Shredding of PHI
    d. Use of surge-protectors

14. Technical safeguards include which of the following?
    a. Encryption of data
    b. Computer system log-ins and passwords
    c. Anti-virus software and firewalls
    d. Information technology (IT) certification review
    e. All of the above
15. “Safe” computing includes which of the following?

a. Sharing passwords with other staff members
b. Remaining “logged on” always, to save time
c. Using email and the Internet ONLY as allowed by practice protocols
d. Installing personal software on the computer