Protecting Patient Privacy
A Training Program for the Medical Office Staff

Revised September 13, 2013
# Contents

Objectives .................................................................................................................. 3

Introduction .................................................................................................................. 3

Frequently Asked Questions ....................................................................................... 4

Case Examples of Possible HIPAA Breaches/Violations ............................................. 16

Risk Management ....................................................................................................... 16

Test Your Knowledge .................................................................................................. 18

Answer Key/Explanations ............................................................................................ 22
A Learning Module for the Medical Office Staff

Objectives

At the conclusion of this learning activity the participant will:

- Understand the personal responsibility related to confidentiality of protected health information
- Identify strategies for protecting confidential patient information common in the work environment.

Introduction


“Much has changed in health care since HIPAA was enacted over fifteen years ago,” said HHS Secretary Kathleen Sebelius. “The new rule will help protect patient privacy and safeguard patients’ health information in an ever expanding digital age.” The changes in the final rulemaking provide the public with increased protection and control of personal health information. (U.S. Department of Health and Human Services. 2013).

These regulations require special attention and handling of patient care information and records (called “protected health information” in the regulations). They require healthcare providers to adopt administrative procedures to advise patients of its privacy practices and their rights with respect to their protected health information (PHI); to designate a person on staff as a contact person for privacy concerns; and to train employees to comply with the regulations governing the electronic transmission of billing data, formats, and codes.

The HIPAA Privacy Rule sets the standards for how to maintain the privacy of personal information in all forms. The focus of this rule is on confidentiality. The Security Rule defines standards for safeguards of personal information, specifically related to electronic protected health information (e-PHI).

To comply with the Privacy Administrative Requirements, medical offices are required to:

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

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

**Why Does Privacy & Security Matter?**

Your patients trust you. Trust is clinically important and a key business asset. How your practice handles patient information is an important aspect of this trust. Protecting the privacy and security of patient information is also an important part of enterprise risk management. Enterprise risk management (ERM) in healthcare promotes a comprehensive framework for making risk management decisions which maximize value protection and creation by managing risk and uncertainty and their connection to total value.” (American Society for Healthcare Risk Management)

In this learning module, we will, answer some of the most frequently asked questions related to the HIPAA Privacy and Security Rules, present several case examples of breaches, and offer risk management tips to enhance compliance.

**Frequently Asked Questions**

**What are the Administrative Requirements?**

• Developing and implementing written privacy policies
• Designation of a privacy official and a contact person responsible for receiving complaints and providing individuals with privacy practices
• Training of all workforce members on its privacy policies
• Mitigating any harmful effect that was knowingly caused by disclosure of PHI
• Implementing safeguards, such as shredding documents before discharging them
• Developing procedures for allowing individuals to complain about its privacy policy and informing the patient that complaints can be submitted to HHS
• Not requiring a patient to waive privacy rights as a condition of obtaining treatment
• Maintaining the privacy policy and procedures, privacy practice notices, and disposition of complaints for six years.

**Who is required to follow the HIPAA law?**

The Administrative Simplification standards adopted by Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) apply to any entity that is:
• a health care provider that conducts certain transactions in electronic form (called here a "covered health care provider").
• a health care clearinghouse.
• a health plan.

An entity that is one or more of these types of entities is referred to as a "covered entity" in the Administrative Simplification regulations (Centers for Medicare & Medicaid Services).

**What are your obligations?**

You are required by law to:

- Maintain the privacy of protected health information
- Give notice of your legal duties and privacy practices regarding health information to each patient
- Follow the terms of your notice that is currently in effect

**What information is protected?**

- Information doctors, nurses and other health care providers put in the medical record.
- Conversations about patient care with other providers
- Health information in a health plan’s computer system

**What are some examples of PHI?**

- Name
- Address (including street, city, county, zip code)
- Name of employer
- Andy date (birth date, encounter date)
- Telephone and FAX numbers
- Email addresses
- Social Security Number
- Medical records

**What is the “minimum necessary standard”?**

The minimum necessary standard is a key protection of the HIPAA Privacy Rule. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires you to evaluate your practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.
Are there any exceptions to the minimum necessary standards?

Yes. Minimum necessary is **not** required for the following:

- Requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Disclosures made pursuant to an individual’s authorization.
- Disclosures to the Department of Health and Human Services (HHS)
- Uses or disclosures that are required by other law

(U.S. Department of Health and Human Services)

**Under what circumstances can PHI be shared?**

**For Treatment.**
You may use and disclose Health Information to coordinate treatment with other health care providers. For example, you may disclose Health Information to doctors, nurses, technicians, or other personnel, including people outside your office who are involved in your patient’s medical care.

**For Payment**
You may use and disclose Health Information so that you or others may bill and receive payment from an insurance company or a third party for the treatment and services you received. For example, you may give the patient’s health plan information so that they will pay for your patient’s treatment.

**For Health Care Operations**
You may use or disclose, as-needed, protected health information in order to support the business activities of the practice. These activities include, but are not limited to, quality assessment, employee review, training of medical students, licensing, fundraising, and conducting or arranging for other business activities. For example, you may disclose your protected health information to medical school students that see patients at your office. In addition, you may use a sign-in sheet at the registration desk where the patient is asked to sign in. You may also call the patient by name in the waiting room when the physician is ready to see them.

**Appointment Reminders, Treatment Alternatives and Health Related Benefits and Services**
You may use and disclose Health Information to contact the patient to remind them of a patient. You can use and disclose Health Information to tell you the patient about treatment alternatives or health-related benefits and services that may be of interest to them.
**Individuals Involved in Your Care or Payment for Your Care**

When appropriate, you can share Health Information with a person who is involved in your patient’s medical care or payment for your care, such as a family or a close friend. You can notify the patient’s family about their location or general condition or disclose such information to an entity assisting in a disaster relief effort.

**Research**

Under certain circumstances, you may use and disclose Health Information for research. For example, a research project may involve comparing the health of patients who received one treatment to those who received another, for the same condition. Before you use or disclose Health Information for research, the project will go through a special approval process. Even without special approval, you may permit researchers to look at records to help them identify patients who may be included in their research project or for other similar purposes, as long as they do not remove or take a copy of any Health Information.

**As Required by Law**

You can disclose Health Information when required to do so by international, federal, state or local law.

**To Avert a Serious Threat to Health or Safety.**

You may use and disclose Health Information when necessary to prevent a serious threat to the patient’s health and safety or the health and safety of the public or another person. Disclosures, however, should be made only to someone who may be able to help prevent the threat.

**Business Associates.**

You can disclose Health Information to your business associates that perform functions on your behalf or provide you with services if the information is necessary for such functions or services. For example, you may use another company to perform billing services on our behalf. All of your business associates are obligated to protect the privacy of your information and are not allowed to use or disclose any information other than as specified in your contract.

**Organ and Tissue Donation.**

If your patient is an organ donor, you may use or release Health Information to organizations that handle organ procurement or other entities engaged in procurement, banking or transportation of organs, eyes or tissues to facilitate organ, eye or tissue donation and transplantation.

**Military and Veterans**

If the patient is a member of the armed forces, you may release Health Information as required by military command authorities.
Workers’ Compensation
You may release Health Information for workers’ compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public Health Risks
You may disclose Health Information for public health activities. These activities generally include disclosures to prevent or control disease, injury or disability; report births and deaths; report child abuse or neglect; report reactions to medications or problems with products; notify people of recalls of products they may be using; a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and the appropriate government authority if you believe a patient has been the victim of abuse, neglect or domestic violence.

Health Oversight Activities
You may disclose Health Information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Data Breach Notification Purposes
You may use or disclose your patient’s Protected Health Information to provide legally required notices of unauthorized access to or disclosure of your health information.

Lawsuits and Disputes.
You can disclose Health Information in response to a court or administrative order. You can disclose Health Information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell the patient about the request or to obtain an order protecting the information requested.

Law Enforcement.
You can release Health Information if asked by a law enforcement official if the information is: (1) in response to a court order, subpoena, warrant, summons or similar process; (2) limited information to identify or locate a suspect, fugitive, material witness, or missing person; (3) about the victim of a crime even if, under certain very limited circumstances, we are unable to obtain the person’s agreement; (4) about a death we believe may be the result of criminal conduct; (5) about criminal conduct on our premises; and (6) in an emergency to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

Coroners, Medical Examiners and Funeral Directors.
You can release Health Information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. You can also release Health Information to funeral directors as necessary for their duties.

**National Security and Intelligence Activities**
You may release Health Information to authorized federal officials for intelligence, counter-intelligence, and other national security activities authorized by law.

**Protective Services for the President and Others**
You may disclose Health Information to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or to conduct special investigations.

**Inmates or Individuals in Custody**
If the patient is an inmate of a correctional institution or under the custody of a law enforcement official, you may release Health Information to the correctional institution or law enforcement official.

**What disclosures require written authorization from the patient?**
- Uses and disclosures for marketing purposes.
- Uses and disclosures that constitute the sales of medical information.
- Most uses and disclosures of psychotherapy notes, if you maintain psychotherapy notes.
- Any disclosure not described in the Notice of Privacy Practices.

**What rights do patients have related to their medical information?**
**The patient has a right to:**

- A paper copy of the Notice of Privacy Practices.
- Access, inspect and copy medical record.
- An electronic copy of the medical record if you maintain records in the electronic format.
- Request an amendment if health information is incorrect or incomplete.
- Obtain a report on when and why their health information was shared.
- Request a restriction or limitation of health information shared with others.
- Request that you not bill their health plan for paid in full out-of-pocket payments (If a Medicare beneficiary requests a restriction on the disclosure of PHI to Medicare for a covered service and pays out of pocket for the service, the provider must also restrict the disclosure of PHI regarding the service to Medicare).
- Request confidential communications.
- To be notified on a breach of unsecured protected health information.
- To opt-out of fundraising and marketing communications.
- To file a complaint.
What is a Notice of Privacy (NPP)?

Every patient should be provided with a copy of the provider’s NPP. The Notice must explain how protected health information is used and disclosed for Treatment, Payment, and Health Care Operations, including examples of each.

The NPP should also explain how protected health information may be disclosed without a patient’s knowledge or consent for purposes other than treatment, payment or health care operations, including meeting the various public health reporting obligations imposed on providers or in response to a court order.

The NPP must be posted in a clear and prominent location with copies of the NPP available for the individual to easily take one. It would not be appropriate for an individual to have to ask the receptionist for a full copy of the NPP. (American Health Information Management Association).

What information is required in the Notice of Privacy Practices?

This Notice must:

- describe the ways the physicians may use and distribute protected health information;
- state the physician’s duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice;
- describe the individual’s rights; and
- provide a point of contact for further information.

Physicians must make a good faith effort to obtain written acknowledgment from patients of receipt of the privacy notices.

Am I required to have the patient sign an acknowledgement that they have received the notice of privacy?

Upon receipt of the Notice of Privacy Practices, the patient should sign an “Acknowledgement of Receipt of Privacy Practices” or, if the patient refuses to sign the acknowledgement, your staff should sign and place a form in the patient’s medical record noting that it was offered and refused. Explain to the patient that signing the acknowledgement does not mean that he/she is agreeing to any special uses or disclosures of his/her health information.

What are the elements of a properly executed authorization?

When releasing PHI for purposes other than treatment, payment and health care operations (TPO), the patient’s written authorization must be obtained in
compliance with the federal privacy standards established by HIPAA. A conforming authorization must meet the following standards:

1) The authorization must be in plain English.
2) It must clearly identify the patient.
3) It must clearly identify who may receive the PHI.
4) If information about drug or alcohol abuse, HIV status or psychiatric records will be released, the release must say so explicitly.
5) The authorization must specify an expiration date or an expiration event.
6) The authorization must identify who may use or release the PHI
7) There must be a warning to the effect that information released pursuant to an authorization may no longer enjoy federal privacy protection.
8) It must state the patient’s rights including the right to revoke the authorization and the right to treatment even if the authorization is not signed.

Do I need a written authorization if I am releasing the information directly to the patient?

You do not need a patient’s written HIPAA Authorization to release medical information directly to the patient, but you do need a signed, dated request from the patient. You should never release the original medical record. The patient owns the information, but the health care provider owns the record and has a duty to safeguard it.

Does the HIPAA Privacy Rule allow us to discuss a patient’s health status, treatment or payment arrangements with the patient’s family and friends?

Yes. The HIPAA Privacy Rule permits you to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient’s care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, you may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. You may also share relevant information with the family and these other persons if it can be reasonably inferred, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient’s mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient’s payment options with her adult daughter.
• A doctor may instruct a patient’s roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
• A physician may discuss a patient’s treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

(U.S. Department of Health and Human Services)

Can I release records that were created by other providers?

If written authorization specifies that “all information” found in the record should be released, you should literally comply with the request, even if other medical providers created portions of the record. If there are portions of the record that you believe in your professional judgment may harm the patient or someone else, you may withhold that portion of the record, subject to a patient’s right to appeal your decision.

See http://www.hhs.gov/ocr/privacy/hipaa/faq/minimum_necessary/214.html

Does the Privacy Rule’s minimum necessary restrictions prevent or hinder necessary exchanges of patient medical information to those involved in the treatment of the patient?

No. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the minimum necessary requirements.

The Rule recognizes that those involved in the care of the patient are in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. You may develop role-based access policies that allow health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.

(U.S. Department of Health & Human Services)

For further guidance see:
http://www.hhs.gov/ocr/privacy/hipaa/faq/minimum_necessary/208.html

Does HIPAA extend extra protections to any category of health information?

Psychotherapy notes” is one category of health information for which HIPAA currently extends “extra” protections, with a requirement for separate authorization. Psychotherapy notes are defined as notes prepared by a mental
health professional concerning counseling sessions with an individual or a group. Practices should keep these notes separate from the patient’s other mental health treatment information to avoid inadvertent disclosure. State statutes typically carve out exceptions and special requirements for genetic information, pregnancy-related information, AIDS and sexually-transmitted disease information. Check the specific statutes for your state.

Can a provider deny access to a patient’s record?

A provider may deny access to his/her patient’s records in certain situations, such as when the provider believes access could cause harm to the patient or another. In such cases, the patient must be given the right to have such denials reviewed by a licensed healthcare provider for a second opinion. Reference: 45 CFR § 164.524.

Can a patient request that certain information be amended if the information is inaccurate or incomplete?

The Privacy Rule also gives patients the right to request that certain information be amended if the information is inaccurate or incomplete. Reference: 45 CFR § 164.526. The Rule provides for a specific process for requesting and responding to a request for an amendment.

If a patient feels that their rights have been violated where can they file a complaint?

They can file a complaint with the privacy officer in your practice or file a complaint with the US Government – Office of Civil Rights.

Do HIPAA laws apply to employee health records?

HIPAA privacy and security rules do not apply to employee health records, however, these records should be treated as confidential and access to these records should be limited.

When are business associate agreements required?

The practice must have a written business associate agreement with outside parties that are engaged to conduct activities or services on its behalf that creates, receives, maintains, or transmits PHI.

Some examples of business associates include

- Accreditation organizations that you may share protected health information with
- A software company that hosts software containing patient information on its own server or accesses patient information.

Can I contact a patient for the purpose of fundraising?
A statement must be included in the Notice of Privacy Practices (NPP) that a you may contact them about fundraising. The recipient of any fundraising communication must be provided with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications and that the individual’s choice to opt out is treated as a revocation of authorization under the Privacy Rule. You can not condition treatment or payment because of an individual’s choice about receiving fundraising communications. The opportunity to opt out of receiving further fundraising communications must be provided with each fundraising communication made.

**What if patient requests a copy of the medical record in an electronic format?**

You must provide an electronic copy of protected health information that is maintained electronically in the form and format requested by the patient. If the form and format are not readily producible, then the information must be produced in an electronic form as agreed to by the you and the patient. If the patient declines any of the electronic formats that are available, the you can provide a hard copy as an option to fulfill the request (American Health Information Management Association).

**Can I honor a patient requests that I email records in an unencrypted format?**

You may send individuals unencrypted e-mails if they have advised the individual of the risks and the individual still prefers that method of delivery (American Health Information Management Association).

**Do I have more than 30 days to respond to a request for medical records if the records are maintained off site?**

You have 30 days with a one-time 30 day extension to respond to the request (with the written notice to the individual of the reasons for delay and expected completion date). This provision extends the 30-day time limit with a one-time 30-day extension to respond to requests for electronic access. This aligns the time period to respond, no matter the location or the media.

**What is a considered a “breach”?**

An impermissible use or disclosure of PHI is presumed to be a breach unless you or your business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised (American Health Information Management Association)
Do I have to notify the patient of a breach only if there is a risk of harm?

The Office of Civil Rights has removed the harm standard and modified the risk assessment to focus more objectively on the risk that the PHI has been compromised.

Thus, breach notification is not required under the final rule if a covered entity or business associate, as applicable, demonstrates through a risk assessment that there is a low probability that the PHI has been compromised, rather than demonstrate that there is no significant risk of harm to the individual as was provided under the interim final rule (American Health Information Management Association).

If a breach occurs, what factors must I consider to determine whether there is a low probability that PHI has been compromised?

To determine whether there is a low probability that PHI has been compromised, the covered entity or business associate must conduct a risk assessment that considers at least each of the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom the disclosure was made.
- Whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

If a breach occurs, how long do I have to notify the patient?

You must notify affected individuals of a breach without unreasonable delay but in no case later than 60 calendar days from the discovery of the breach, except in certain circumstances where law enforcement has requested a delay. The time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete. You are expected to notify individuals as soon as reasonably possible after the covered entity takes reasonable time to investigate and collect information to be included in the notification. Keep in mind that 60 days is the outer limit (American Health Information Management Association).

Notify your insurance insurance carrier if your policy provides coverage for a HIPAA breach.

What if the breach affects more 500 or more patients?

You must report breaches affecting 500 or more individuals to the Office of Civil Rights (OCR) immediately. “Immediately” is interpreted to require that
notification be sent to the OCR at the same time that the notification is sent to the individual. (American Health Information Management Association).

**Case Examples of Possible HIPAA Breaches/Violations**

A Practice Manager has an employee who has developed a pattern of tardiness and declining work performance. The employee is a patient of the practice and has seen one of the physicians in the practices several times recently. The Practice Manager accessed the employee’s medical record to see if she can find out if a medical problem is affecting the employee’s work performance.

An unencrypted portable media device containing PHI is left in a rental car and is not recovered.

An employee is curious about his or her neighbor who is a patient at the practice and accesses the patient’s medical record then shares with friends.

An eighteen year old patient visits her OB/GYN physician. She specifically indicated that nothing about her condition or treatment was to be discussed with her parents. The patient is given pregnancy test during the visit. The patient is covered under her mother’s insurance and payment for the visit is submitted to the insurance company. Upon reviewing the bill that only includes diagnosis codes and charges, the mother calls the business office and asked what the codes mean. After learning that the code was for a pregnancy test, the mother wants to know if her daughter is pregnant. The business office personnel explain the bill to the mother and tell her the results of the test.

An employee posts information about a patient on a social media site such as Facebook or Twitter.

PHI is faxed to the wrong number outside of the covered entity.

PHI has been changed or destroyed in an unauthorized manner.

**Risk Management**

**Basic Privacy Tips**

1. Look at a patient’s PHI only if you need it to perform your job.
2. Use a patient’s PHI only to the extent that is required to perform your job.
3. Give a patient’s PHI to others only when it’s necessary for them to perform their jobs.
4. Talk to others about a patient’s PHI only if it is necessary to perform
7. your job, and do it discreetly.
8. Assign computer access levels based on job responsibilities.

**Basic Security Guidelines**

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

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

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

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

• **Malware** – protect against viruses, spyware, and worms that could compromise security, avoid suspicious email (American Academy of Professional Coders Physician Services)

Disclaimer:
This learning module does not constitute a legal opinion, does not establish any standards of care and is current as of September 2013. Physicians who encounter problems in any of these areas should seek a qualified legal opinion from a licensed attorney.

References

American Health Information Management Association. *Analysis of modifications to the HIPAA privacy, security, enforcement and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other modifications to the H.* Chicago, IL: American Health Information Management Association, 2013.


---

**Test Your Knowledge**

**HIPAA Compliance in the Medical Office Setting**
Question 1
The HIPAA law requires the medical practice to designate a person on staff as a contact person for privacy concerns and to train employees to comply with the regulations governing the electronic transmission of billing data, formats, and codes.

☐ True ☐ False

Question 2
A doctor who refers a patient to a specialist may discuss the case with the specialist without violating the patient's rights.

☐ True ☐ False

Question 3
A patient has the right to review and obtain a copy of their medical record.

☐ True ☐ False

Question 4
If a patient requests an amendment to their medical record, the physician is required to make the requested change.

☐ True ☐ False

Question 5
A provider may deny access to a patient’s record in certain situations, such as when the provider believes the access could cause harm to the patient or another.

☐ True ☐ False

Question 6
An authorization is not valid unless it contains all of the required elements and statements.

☐ True ☐ False

Question 7
A patient may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that practice has taken action based on the authorization and prior to notice of revocation.

☐ True ☐ False

**Question 8**
Only written information in the medical record is considered protected health information.

☐ True ☐ False

**Question 9**
If a patient complains about a privacy breach and the privacy officer is out of the office, tell them to call the Office of Civil Rights.

☐ True ☐ False

**Question 10**
A patient can request a restriction on the disclosure of his/her protected health information?

☐ True ☐ False

**Question 11**
If a patient requests that I email a copy of their medical record in an unencrypted format, I am permitted to send it after I explain the risks.

☐ True ☐ False

**Question 12**
If a patient has paid for services out of pocket and in full, they can instruct us not to share information about their treatment with their health plan.

☐ True ☐ False

**Question 13**
If a patient is a Medicare recipient and has paid for services out of pocket and in full, we are not allowed to honor a request to restrict information about their treatment with Medicare.

☐ True ☐ False

**Question 14**
I can sell an individuals/health information without their permission.

☐ True ☐ False

**Question 15**
I only have to report a breach to a patient if I think he/she could be harmed because the information was accessed/disclosed.

☐ True ☐ False
Answer Key/Explanations

Question 1
The HIPAA law requires the medical practice to designate a person on staff as a contact person for privacy concerns and to train employees to comply with the regulations governing the electronic transmission of billing data, formats, and codes.

☐ True     ☐ False

Answer/Explanation: True. HIPAA's Privacy Rule requires the designation of a "privacy official" by each covered entity, to be responsible for the "development and implementation" of the policies and procedures necessary for compliance.

Question 2
A doctor who refers a patient to a specialist may discuss the case with the specialist without violating the patient's rights.

☐ True     ☐ False

Explanation: True. A physician may always disclose protected health information to another physician or other health care provider for treatment. The physician does not need to limit or otherwise restrict the amount of information disclosed for purposes of treatment.

Question 3
A patient has the right to review and obtain a copy of their medical record.

☐ True     ☐ False

Explanation: True. HIPAA's Privacy Rule grants every individual a "right of access" -- to inspect and obtain a copy of all protected health information within the designated record set maintained by the covered entity.

Question 4
If a patient requests an amendment to their medical record, the physician is required to make the requested change.

☐ True     ☐ False

Explanation: False. HIPAA's Privacy Rule grants individuals a "right to amend" -- that is, to take exception to information in their records with which they disagree, and request corrections. Covered entities may choose to make requested changes; or the information can be left unchanged if it is believed to be correct, but with documentation in the record of the patient's disagreement. (A right to
amend exists, in varying forms, under the laws of many states. HIPAA makes it national.)

**Question 5**
A provider may deny access to a patient’s record in certain situations, such as when the provider believes the access could cause harm to the patient or another.

- [ ] True
- [ ] False

Explanation: True. A denial of access is permissible, but with an opportunity to appeal, when a “licensed health care professional, in the exercise of professional judgment” determines that the requested access is “reasonably likely” to endanger the life or physical safety of, or cause substantial harm to, the individual or another person. Requests by a personal representative of an individual may be denied for the same reasons.

**Question 6**
An authorization is not valid unless it contains all of the required elements and statements.

- [ ] True
- [ ] False

Explanation: True. The regulations generally prohibit the disclosure of information unless all required elements of the authorization are present.

**Question 7**
A patient may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that practice has taken action based on the authorization and prior to notice of revocation.

- [ ] True
- [ ] False

Explanation: True. An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that the covered entity has taken actions relying on it. (See especially the discussion of such revocations in the context of research.)

**Question 8**
Only written information in the medical record is considered protected health information.

- [ ] True
- [ ] False
Explanation: False. The Privacy Rule also reaches to data transmitted or maintained in any other form or medium." That includes paper records, fax documents and oral communications.

**Question 9**
If a patient complains about a privacy breach and the privacy officer is out of the office, tell them to call the Office of Civil Rights.

☐ True    ☐ False

Explanation: False. HIPAA requires that every covered entity have an internal process for receiving and evaluating complaints of HIPAA violations. Typically, such complaints will be the responsibility of the privacy office/officer designated by the organization.

Individuals who believe that a covered entity is not complying with HIPAA requirements may also file a complaint with the Secretary of the federal Department of Health and Human Services (DHHS). Currently the Office of Civil Rights (OCR) within DHHS has been designated to receive such complaints. It is preferable that the issue be resolved internally whenever possible.

**Question 10**
A patient can request a restriction on the disclosure of his/her protected health information?

☐ True    ☐ False

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

**Question 11**
If a patient requests that I email a copy of their medical record in an unencrypted format, I am permitted to send it after I explain the risks.

☐ True    ☐ False

Explanation: True. You may send individuals unencrypted e-mails if they have advised the individual of the risks and the individual still prefers that method of contact.

**Question 12**
If a patient has paid for services out of pocket and in full, they can instruct us not to share information about their treatment with their health plan.

☐ True  ☐ False

Explanation: True. Under the final rule, when patients pay out of pocket in full, they can instruct their provider to refrain from sharing information about their treatment with their health plan.

**Question 13**
If a patient is a Medicare recipient and has paid for services out of pocket and in full, we are not allowed to honor a request to restrict information about their treatment with Medicare.

☐ True  ☐ False

Explanation: False. Under the final rule, when patients pay out of pocket in full, they can instruct their provider to refrain from sharing information about their treatment with their health plan. If a Medicare beneficiary requests a restriction on the disclosure of PHI to Medicare for a covered service and pays out of pocket for the service, the provider must also restrict the disclosure of PHI regarding the service to Medicare.

**Question 14**
I can sell an individuals/health information without their permission.

☐ True  ☐ False

Explanation: False. The Final Rule prohibits the sale of an individuals' health information without their permission.

**Question 15**
I only have to report a breach to a patient if I think he/she could be harmed because the information was accessed/disclosed.

☐ True  ☐ False

Explanation: False. The Office of Civil Rights has removed the "harm" standard in the Final Rule and modified the risk assessment to focus more objectively on the risk that the PHI has been compromised.

Thus, breach notification is not required under the final rule if a covered entity or business associate, as applicable, demonstrates through a risk assessment that there is a low probability that the PHI has been compromised, rather than demonstrate that there is no significant risk of harm to the individual as was
provided under the interim final rule (American Health Information Management Association).