**Module 4**

**Electronic Health Record Security and Privacy**

**Acknowledgements**

This curriculum was developed with grant funding from The Healthcare Workforce Transformation Fund through the Commonwealth of Massachusetts, Executive office of Labor and Workforce Development. The grant project was administered by Commonwealth Corporation and The Massachusetts eHealth Institute.



**Being an effective presenter:**

Knowing how to lecture well is a crucial skill to master. Effective lecturing is characterized by enthusiasm and expressiveness, clarity, and interaction (Murray in Perry & Smart, 1997). Consider using the tips below to introduce students to the subject and stimulate their enthusiasm about the course material.

* **Be Prepared**
	+ Outline clear objectives for your lecture—both what students should know after the lecture and why it is important.
	+ Develop a lecture outline and any audiovisuals.
	+ If you are nervous about the lecture, write out your introduction and rehearse it.
* **Keep Your Focus**
	+ Create effective visuals, analogies, demonstrations, and examples to reinforce the main points.
	+ Share your outline with students.
	+ Emphasize your objectives and key points in the beginning, as you get to them, and as a summary at the end.
* **Engage Your Audience**
	+ Focus attention early on using a quote, a dramatic visual, an anecdote, or other material relevant to the topic.
	+ Integrate visuals, multimedia, discussion, active learning strategies, small-group techniques, and peer instruction.
	+ Link new material to students’ prior knowledge, such as common experiences or previous coursework.
	+ Show enthusiasm for the topic and information. Remember, you are modeling your discipline.
	+ Give students time to think and genuine opportunities to respond.
	+ Plan for diverse learners. Use verbal, visual, and kinesthetic approaches such as hands-on exercises and simulations.
* **Get Feedback**
	+ Observe students’ non-verbal communication: notetaking, response to questions, eye contact, seating patterns, and response to humor. Are they “with” you?

**Module 4: Electronic Health Record Security and Privacy**

**Introduction**

Security and privacy are vital when handling patient information in Electronic Health Records (EHRs). Specific to protecting the information stored in EHRs, the HIPAA Security Rule requires that health care providers set up physical, administrative, and technical safeguards to protect your health information.  This module will focus on best practices of securing EHRs and protecting patient’s privacy.

**Module 4: Electronic Health Record Security and Privacy**

**Learning Outcomes** (Slide #3)

Upon completion of this course the learner will be able to:

* Discuss the HIPAA’s Privacy &. Security Rules
* List specific types of identifying information that need to be kept secure
* Give examples of the Administrative, Physical, and Technical safeguards that help to protect sensitive patient information
* Understand compliance plans and policies, data breaches

**Module 4: Electronic Health Record Security and Privacy**

**Syllabus**

Lesson 1: Privacy and Security

* Health Insurance Portability and Accountability Act HIPAA
* Privacy vs. Security Rule
* Covered Entities & Business Associates
* Protected Health Information (PHI) and Electronic Protected Health Information (ePHI)
* Individually Identifiable Health Information (IIHI)
* Minimum Necessary Standard

Lesson 2: Privacy Rule

Lesson 3: Security Rule: Administrative, Physical & Technical Safeguards

* General Rules
* Components, Policies and Procedures

Lesson 4: Compliance Plans & Policies

Lesson 5: Fines & Penalties

* Data Breach
* Consequences

**Module 4: Electronic Health Record Security and Privacy**

**Instructor Teaching Points**

**Lesson 1: Privacy and Security**

**What is HIPAA?** (Slide # 4)

An Act is a Law, HIPAA was enacted in 1996 and was implemented in 2003. It standardized how all patient information, in media (oral, written, electronic) can be used, disclosed, maintained and transmitted.

The Law is:

* An extension of doctor-patient confidentiality.
* Allows access to personal and confidential information (essential to accurately reporting data).
* Protects protected health information (PHI) in any form
* Protects individually identifiable health information regardless.
* Portability allows employees, upon termination, the ability to continue their health insurance coverage usually at the full cost of the policy, for at least 18 months until they are able to get coverage from another employer. This assists the employee to have continued coverage to bridge the gap between jobs.
* Accountability requires that all Covered Entities and Business Associates comply with the Law and are accountable.

The Privacy Rule not only takes into account uses and disclosures of patient information but also gave patients rights about the healthcare information, including;

* Receive a notice of the privacy practices – “HIPAA Policy”
* To see their PHI and get a copy
* See the disclosures that have been made of their PHI – Accounting of Disclosures
* To request that changes be made to correct errors in their records or to add information
* To request that their PHI has restricted access
* To file a complaint if they feel their patient information has been breached

The Security Rule is not a one-time project, but rather an on-going, dynamic process that will create new challenges as covered entities’ organizations and

technology changes.

*Ask the class if they are aware of any new technologies that may have an impact on an organization’s ability to comply with the privacy or security rule; i.e social media, telehealth/telemedicine, on line doctor’s visits*

**Privacy vs. Security** (Slide #5)

Privacy refers to not using or disclosing patient information without the patient’s authorization, expect for reasons of treatment, payment and healthcare operations.

*Ask the class why it is important for patients to have their PHI kept private and confidential. What if you, as a patient, did not feel your information was going to be kept private, for example you recognize someone in the office as your neighbor. Would this prevent you from disclosing everything to your provider…even if it may be embarrassing??*

Security addresses how we protect patient information from unauthorized access.

**Privacy Rule vs. Security Rule** (Slide #6)

The Privacy Rule not only takes into account uses and disclosures of patient information but also gave patients’ rights about the healthcare information.

Define use of patient information - Information is shared between people who work together in the same office and need to exchange PHI in order to better serve the patient.

Define disclosure of patient information - PHI is revealed to someone outside the healthcare office or facility in order to better serve the patient.

The Security Rule is not a one-time project, but rather an on-going, dynamic process that will create new challenges as covered entities’ organizations and technology changes.

The HIPAA Security Rule requires Covered Entities to establish safeguards to protect PHI

* + Encryption—method of converting a message into encoded text as data in transmitted or stored
	+ Security Measures
		- Secure Internet connections
		- Access control, password (confidential authentication information = the key), and log files
		- Backups
		- Security policies

*Ask the class if they are aware of any new technologies that may have an impact on an organization’s ability to comply with the privacy or security rule; i.e social media, telehealth/telemedicine, on line doctor’s visits*

**Covered Entities** (Slide #7)

The organizations that must be compliant with HIPAA.

* Healthcare providers
	+ Physicians, hospitals, laboratories, pharmacies, etc.
* Health plans
	+ Medicaid, Medicare, Blue Cross Blue Shield, Tricare, etc.
* Healthcare clearinghouses – facilitate transmission of claim data and reimbursement, eligibility responses
	+ National Clearinghouse, NDC Electronic Claims

**Business Associates** (Slide #8)

*Ask the class if they can think of any other business associates that may have access to PHI – outside cleaning service, outside IT company, drug representatives*

The Covered Entity must have a signed business associates agreement with any non-employee company that may have access to patient information in any form. This outlines to the Business what the organization’s expectations are able the BA’s access to PHI and that the Business Associate and their employees are also liable if there is a data breach.

**PHI and ePHI** (Slide #9)

HIPAA protects an individual’s health information and his/her demographic information.

This is called “protected health information” or “PHI”, in an electronic format it is referred to as “EPHI”.

* PHI/EPHI consists of:
	+ Health information related to past, present, or future physical or mental health of the individual.
	+ Descriptions of a disease, diagnosis, procedure, prognosis, or condition of the individual and can exist in any voicemail, email, fax or verbal or written communications.

**Individually Identifiable Health Information** (Slide #10)

*Ask students how these items could identify a patient*

* *Names*
* *Dates relating to patient*
* *Telephone numbers, addresses, contacts*
* *Social security numbers*
* *Medical record numbers*
* *Photographs*
* *Finger and voice prints*
* *Any other unique identifying number – their insurance policy number*

**Minimum Standard Rule** (Slide #11)

Minimum necessary standard—principle of using reasonable safeguards to disclose PHI only to the extent needed.

*Provide a scenario to illustrate sharing minimum information – PCP is seeing a patient for an annual exam, she believes the patient may be suffering from a respiratory condition. The patient also had a broken femur last year, gout the year before and cataract surgery the year before that. This patient has been coming to this office for 10 years. Is the entire chart released to the pulmonologist? Why or Why not? If so what should be sent. Answer: Only those notes that are related to the PCP’s concern about potential respiratory issues.*

**Lesson 2: Privacy Rule**

**Patient Rights** (Slide #12)

Ask students if they are routinely offered the HIPAA policy when they are a new patient. Have any of them ever read it? If available, give the students a sample NPP and go discuss it in class.

Many patient rights were standardized with the implementation of HIPAA.

Some of the rights are:

Receiving a copy of the organization’s Notice of Privacy Practices which provides:

* Notice about how their health information will be used and disclosed
* Must be written in plain language, preferably in the patient’s primary language
* Must be offered to the patient at their first visit to the facility, if the NPP is updated it must be offered to all patients including established patients
* Must provide the name of the Privacy Officer at the facility who is responsible for education of staff, management of patient complaints and breaches of privacy or data

A copy of the patient’s record must be made available to them within 60 days of request, physicians have the rights to redact any information they deem harmful to the patient.

A patient is entitled to receive an Accounting of Disclosures, which lists any outside organization that their information has been shared with in the last 2 years.

If a patient notices an error in their chart they can request an amendment, in writing, for correction of their record or additional information that needs to be added.

A patient has the right to restrict access to their record both internal to the facility and external of the facility.

If a patient feels there is a breach in their privacy, they have the right to complain to the Privacy Officer of the facility. They can also fie a compliant with the Office of Civil Rights, an agency within the Department of Health and Human Services.

**Lesson 3: Security Rule: Administrative, Physical & Technical Safeguards**

**Security Rule: Administrative Safeguards** (Slide #13)

In general, these are the administrative functions that should be implemented to meet the security standards. These include assignment or delegation of security responsibility to an individual and security training requirements.

*Ask the class what policies & procedures should be in place to ensure your organization is in compliance with the Administrative Safeguard, some examples are as follows:*

* *Continual Risk Analysis and Management of your IT systems – periodically look at your systems to assess weaknesses*
* *Access Authorization – are only people with authorized access getting into your system*
* *Log in Monitoring – proper log in procedures for specific software needs*
* *Password Management – good, secure passwords and frequent changing of passwords*
* *Sanction Policies for Non-Compliance or Breaches – what are the consequences when there is a breach or non-compliance with safeguards*
* *Contingency Plans for Data Back ups, Discovery Recovery – what does the organization do in an emergency to secure all electronic data, and to test data back ups to ensure they are restorable in case of a disaster*
* *Business Associates – those people that are not our employees but may have access to our PHI (i.e. outsourced cleaning staff, outsourced IT, Accountants, Lawyers, etc.) must sign an agreement that they understand their responsibilities with our patient’s health care information.*

**Security Rule: Physical Safeguards** (Slide # 14)

In general, these are the mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion. They include restricting access to EPHI and retaining off site computer backups

*Ask the class what policies & procedures should be in place to ensure your organization is in compliance with the Physical Safeguard, some examples are as follows:*

* *Facility Controls – who has access to the facility and IT areas*
* *Workstation Use – are workstations set up to facilitate employee use*
* *Workstation Security – area monitors protected from view of patients walking by*
* *Device and Media Controls – how do we destroy obsolete IT equipment or reuse IT equipment*

**Security Rule: Technical Safeguards** (Slide # 15)

In general, these are primarily the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing onto a computer is authorized to access that EPHI, or encrypting and decrypting data as it is being stored and/or transmitted.

*Ask the class what policies & procedures should be in place to ensure your organization is in compliance with the Technical Safeguard, some examples are as follows:*

* *Unique User IDs – all users have their own usernames and passwords*
* *Automatic logoff – computers automatically log off previous user after a short period of inactivity*
* *Encryption and Decryption of Data – data cannot be accessed and interpreted as it moves through the Internet*
* *Emergency Access procedures – how can access to database be achieved in an emergency*
* *Entity Authentication – prove that the person entering information is who they say they are*

**Lesson 4: Compliance Plans and Policies**

**Compliance Plans** (Slide #16)

Healthcare organizations must have written compliance plans to address how an organization ensures compliance with regulations:

* Privacy Rule
* Security Rule
* General health information regulations

HIPAA requires a Privacy & Compliance officer(s) to monitor new and existing regulations, handle the reporting of incidents, and educate new and existing staff on a regular basis.

Policies must address all aspects of the Privacy Rule and Security as we have discussed earlier in the presentation.

There also has to be evidence that the organization utilizes monitoring and auditing system for to ensure compliance and identify non-compliance, and to enforce adequate disciplinary sanctions when appropriate.

**Compliance Policies** (Slide # 17)

Notice of Privacy Practices – as discussed earlier this is an important document that must be offered to all new patients

Shredding – any piece of paper that had identifiable information on it must be shredded, not thrown in the trash

*Ask the class if a payment envelope received at the office with the patient’s name on it should be shredded? Or a piece of scratch paper or post it note with IIHI on it. Yes!*

Computer monitors should not face any public areas or areas that the public is walking though. Protection screens should be used to cover monitors and timeouts should be used to automatically log off the user after a period of inactivity, 1 – 2 minutes

**Compliance Policies (continued)** (Slide #18)

All paper records should not be placed where the public can easily see them.

*Ask the class if they have ever seen paperwork at the front desk or check out and were able to see other patient names? Discuss what could have been done to prevent this accidental disclosure.*

You are responsible for your work, never share your password with another employee or enter data under another’s account.

*Ask the class why this is important, if they are all entering data on the same patient, why not use the same computer log on???*

If you are given an email account from your employer it is to be used for business only, not for personal use. Limited patient information, if any, should be sent via email since you are unable to ensure that the email address you are sending to is secure.

*Pose this scenario to students: you received a funny email that includes a link from someone you know, you click on the link only to discover that you introduced a virus to your server. Discuss the ramifications of this event; potential damage to patient data, financial record, affecting the ability for software to work properly, may shut down access to server, the time and money spent to get the system cleaned…..*

**Compliance Policies (continued)** (Slide #19)

It is so important to educate all employees about privacy and security protocols within your facility. This should not only occur at orientation but should be an annual training, documented by the facility, to review these important policies and everyone’s role in protecting ad securing patient data. Employees cannot be held to policies and procedures unless they are educated about them.

*Ask the class…if there was a breach and the facility had no record of educating their employees, would that look bad for the facility during an investigation….why or why not?*

Employees should only print patient information when needed to do their job, all print outs must be shredded after their use

Your organization will run security audit to assess all user’s activity in the system, this includes, entering, modifying, deleting data, access to records, printing, faxing, viewing, etc. Security audit should be ran routinely to ensure data integrity. It will definitely be monitored if there is question of a breach.

Your IT department is responsible to keep the server safe and secure by maintaining up to date firewalls (software to protect unauthorized access) and virus protection.

**Compliance Policies (continued)** (Slide #20)

Care must be taken any time patient information is used or disclosed.

Pre-programming faxes numbers to often faxed to facilities may assist with faxing errors,

*Ask students if they have been asked to show an ID at the doctor’s office for an appointment, to pick up a prescription or medical records.*

*Has anyone asked someone else to pick a prescription or medical records, if so were you asked to sign a release and was the person picking up the document asked for identification?*

It seems that most people are on some social media site. You cannot post anything about your patients, your employer, pictures even with the patient’s permission. Social media sites are for your personal life not your professional life, keep them separate.

Your organization will have very specific policies about computer use and social media, take it seriously you may be terminated or worse be fined or go to jail!

Treat a patient’s medical record the way you would want someone to treat your medical record.

**Lesson 5: Data Breaches & Consequences**

**Fines & Penalties** (Slide # 21)

Breach of a patient’s PHI can be in any form, written, oral or electronic.

A breach is when PHI is unsecured and there is a likelihood of use or disclosure without the individual’s permission; could result in: disciplinary action, loss of access privileges, Imprisonment, fines and penalties. If your organization has a breach, it must notify each affected individual within 60 days of discovery of the breach. This is true even if it only affects one individual. Breaches that involve over 500 patients must also be reported to the media.

*Ask the class if they have heard of any breaches of patient information; Anthem BCBS, laptops being stolen from vehicles, etc.*

*Discuss with the class why employees can be held liable, not just the provider or organization.*

**Module 4: Electronic Health Record Security and Privacy**

**Summary** (Slide #22)

You have learned about:

* The Health Information Portability and Accountability Act (HIPAA) - Privacy & Security Rule
* Security and privacy safeguards of the EHR including
	+ Administrative Safeguards
	+ Physical Safeguards
	+ Technical Safeguards
* Data Breaches & Consequences
* Ways in which healthcare workers can protect the privacy of sensitive healthcare information
* Ways in which healthcare workers can secure the EHR

**Module 4: Electronic Health Record Security and Privacy**

**Exam with Answer Key**

1. Who does HIPAA cover?

A. Nursing Homes

B. Healthcare providers that transmit standard transactions electronically

C. Home Health Agencies

D. All of the above

E. None of the above.

Answer: D. All of the above

2. What could happen to a person who knowingly violates patient privacy for personal gain or malicious harm?

1. Disciplinary action
2. Loss of access privileges
3. Fines and penalties
4. Imprisonment
5. All of the Above

Answer: E. All of the Above

3. You're an employee at a Nursing Home. One day, when you're working in the new resident admission office, you see your neighbor, Bill come in as a new resident. Bill's daughter is a friend of yours.

*True or False?* You can call Bill's daughter and let her know you will take good care of her dad?

Answer: False. Instead, disclose to the nursing staff that you know the patient and his daughter. Your friend’s father has a right to privacy. You cannot discuss Bill with anyone not involved in his care.

4. What makes a good password?

1. Using a wide range of characters
2. Using mixed case in words
3. Using mnemonics to help you remember passwords
4. None of the above.
5. All of the above

Answer: E. All of the above

5. If someone forgets their logon ID, can I let them use mine?

1. Yes, if he is an employee and you know him
2. Yes, if your manager says that it’s okay
3. No, sharing logon IDs and passwords is a security violation. The individual should contact the Help Desk for assistance
4. All of the above
5. None of the above

Answer: C. No, sharing logon IDs and passwords is a security violation. The individual should contact the Help Desk for assistance

6. What are some things I can do to be more alert to Privacy and Security?

1. Report incidents
2. Activate screen saver with a password
3. Improve your password strength and don't share it with anyone
4. Do not install unauthorized software
5. All of the above

Answer: E. All of the above

7. Over the past two years, you've collected many, many sheets of paper that contain patient names and other identifiable health information. You’d like to get rid of some of this paper. What should you do?

1. Use it as scratch paper
2. Throw it in the trashcan
3. Destroy it or put it in the secure shred box
4. All of the above
5. None of the above

Answer: C. Destroy it or put it in the secure shred box

8. Health IT security includes?

1. Technical Safeguards
2. Physical Safeguards
3. Administrative Safeguards
4. All of the above .
5. None of the above

Answer: D. All of the above

9. Technical Safeguards include?

1. Access control
2. Audit controls
3. Integrity
4. Transmission security
5. All of the above
6. None of the above

Answer: F. None of the above

10. You're a Nursing Assistant at a Nursing Home. Someone calls and says, "This is… uh… Officer Robert Brown with the… uh… Boston Police Department. I'm looking for Leslie Greenfield. Her son… uh, step-son… no, husband reported her missing. There's plenty of newspaper piled up by her house. He says she is at your nursing home. Is she there now?"

*What should you do?*

Answer: In all cases, unless you know the caller, you are not permitted to disclose any information. Tell the caller, I’m sorry. I am unable to help you over the telephone. Direct the caller to make his request in person at the Nursing Home. He should be prepared to present identification.

**Glossary of Terms**

**Business associate (BA**): Organizations that work for covered entities but are not themselves Covered Entities themselves

**Breach:** Disclosure of protected health information in a manner which compromises the security or privacy of the protected health information.

**Confidentiality:** The practice of permitting only certain authorized individuals to access information that they will only disclose to other authorized individuals as permitted by law. For example, substance abuse information may not be released without specific consent.

**Covered Entity (CE):** Healthcare organization (health plan, clearinghouse, provider, or business associate) that transmits HIPAA-protected information electronically or maintains in any other form, i.e. written, oral

**Health Insurance Portability and Accountability Act (HIPAA):** The federal Health Insurance Portability and Accountability Act of 1996. Its goal is to help the privacy and security of patient's medical records, also known as protected health information (PHI).

**Individually Identifiable Health Information (IIHI):** Any information that could identify a patient, this can be demographic as well as clinical information

**Notice of Privacy Practices:** Informally known as “the HIPAA policy”, this is the document that is given to each new employee which outlines how they will use and disclose patient information as well as how they comply with HIPAA regulations.

**Protected Health Information (PHI):** Individually identifiable health information (medical records, demographics, or payment data) that is transmitted by electronic media.

**Privacy:** An individual’s right to control his or her protected health information.

**Security:** The protections or safeguards put in place to secure protected health information.

**Security Rule:** Assure the confidentiality, integrity, and availability of electronic protected health information.