**Introduction to Health Information Technology:**

 **A Guide for Entry Level Healthcare Professionals**

***Student Handout***

**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.



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

**Syllabus**

Lesson 1: Privacy vs. Security

1. Definitions
2. Privacy vs. Security Rule
3. Protected Health Information (PHI) and Electronic Protected Health Information (ePHI)
4. Covered Entities

Lesson 2: Administrative Safeguards

1. General Rules
2. Components, Policies and Procedures

Lesson 3: Physical Safeguards

1. General Rules
2. Components, Policies and Procedures

Lesson 4: Technical Safeguards

1. General Rules
2. Components, Policies and Procedures

Lesson 5: Fines & Penalties

1. Data Breach
2. Consequences

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

**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.

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

**Exam**

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.

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

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?

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

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

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

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

8. Health IT security includes?

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

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?*