HIPAA Security Training

Updated May 2016
Course Objectives

- This computer-based learning course covers the HIPAA, HITECH, and MSHA Privacy and Security Program which includes relevant Information Technology (IT) security educations.
  - Definitions and Terms
  - HIPAA and HITECH Overview
  - Requirements of the HIPAA Regulations
  - MSHA Workforce Member Responsibilities
  - HIPAA applied to real-life situations
  - Current IT security awareness
Definitions and Terms

- **Access**: The ability to read, write, modify or communicate data/information or otherwise use any system resource.

- **Authentication**: The confirmation that a person is the one claimed.

- **Confidentiality**: When information/data is not made available or disclosed to unauthorized persons or processes.

- **Covered Entity**: Health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

- **Encryption**: A process of changing data into a form where there is a low chance of knowing the meaning without use of a process or key.

- **Malicious Software**: Software (often a virus) designed to damage a system.
Definitions and Terms

- **Password:** Confidential information to allow access and identify the user.

- **Protected Data:** Identifiable patient information, financial, company confidential data.

- **Security incident:** Unauthorized access, use, disclosure, modification or destruction of information or interference with system operations.

- **Security officer:** The individual designated by a covered entity to oversee HIPAA Security Regulation compliance.

- **User:** A person with authorized access.

- **Workstation:** An electronic computing device, such as a laptop or desktop computer, or any device that performs similar functions including any electronic media.
Privacy and Security Laws

- With an increase in the ease of electronic communications and data storage, the federal government recognized a need to establish specific security regulations.
  - These were set forth in the HIPAA Security Rule in 2005.
- In 2009, additional disclosure and security provisions were created, referred to as the HITECH provisions.
- Omnibus legislation changed the burden of proof. No longer are covered entities “innocent until proven guilty,” but a covered entity is “guilty until proven innocent.”
HIPAA Security Rule

- Whereas, the HIPAA Privacy Rule deals with Protected Health Information (PHI) in general, the HIPAA Security Rule (SR) deals with electronic Protected Health Information (ePHI), which is essentially a subset of what the HIPAA Privacy Rule encompasses.

- The Security Rule specifies a series of:
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards

- That covered entities are to use to assure the confidentiality, integrity, and availability of e-PHI.
HIPAA Security Rule

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

• Specifically, covered entities must:
  – Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  – Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  – Protect against reasonably anticipated, impermissible uses or disclosures; and
  – Ensure compliance by their workforce
Administrative Safeguards

- Actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic PHI.

- In general, these safeguards require MSHA to:
  - Maintain processes to address management of security, including:
    - Risk analysis
    - Disciplinary policies
    - System activity review
  - Identify an individual who is responsible for overseeing compliance with the HIPAA Security Rule.
    - At MSHA, this person is HIPAA Compliance Officer in the Corporate Audit and Compliance Services Department.
MSHA must:

- Implement policies/procedures addressing access to electronic PHI.
- Provide training on security processes and practices.
- Implement policies/procedures to address security incidents/violations.
- Establish policies/procedures for contingency plans, data backup, disaster recovery, etc.
- Develop processes to perform periodic evaluations of security processes.
- Include security requirements in appropriate contracts.
Technical Safeguards

- HIPAA Security Rule requires a covered entity to implement technology, policies and procedures to properly address:
  - **Access Control**: A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).
  - **Audit Controls**: A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
  - **Integrity Controls**: A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
  - **Transmission Security**: A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.
Technical Safeguards

- **General safeguards at MSHA:**
  - Implement policies and procedures to allow **access only to those who have the right to such access.**
    - This includes assigning unique user passwords for identifying and tracking user identity.
  - Implement mechanisms that record system **activity/audits.**
  - Implement processes to protect electronic PHI against **improper destruction.**
  - In order to insure security of username and password MSHA users should not use MSHA password on any personal sites.
    - This helps to minimize our exposure to inappropriate third party unknown access to your account.
Technical Safeguards

❖ Use of Personal Devices
  ▪ Use of personal devices to access work applications and work files is not recommended.
    o When a personal device is used to access work applications or work files the device the workforce member is responsible for ensuring the device has up-to-date operating systems, anti-virus and anti-malware software.

❖ Remote Access
  ▪ Access to MSHA computer systems is limited to workforce members who have appropriate work reason and requires approval by appropriate MSHA leaders.
  ▪ Workforce members with remote access are responsible for complying with all MSHA HIPAA Privacy and Security policies.
  ▪ Students generally are not granted remote access.
Passwords

- Passwords are considered a technical safeguard.
- You are responsible for your user ID and passwords and will be held accountable for any access or actions taken using your login ID.
  - Do not share your password.
  - Do not leave a computer you are logged on to unattended.
  - Do not let others access PHI while you are logged on to the computer or application.
  - Do not use your MSHA password on any third party websites.

** Review MSHA policy IM-900-004 Computer Access Codes Management.**
MSHA Electronic Communication

- MSHA has many ways of communicating electronically. It is the Workforce member’s responsibility to keep PHI confidential.
  - **Electronic Mail**
    - Always use secure eMail method if you are sending patient information to a non-MSHA email address.
    - Type [securemail] in the subject line. Never include patient information in the subject line even when sending the email to a MSHA email address.
  - **FAX**
    - Verify all FAX numbers before faxing any patient information.
    - Routinely check auto-fax numbers. Keep faxing to a minimum.
    - Use approved MSHA fax cover sheet with disclaimer.
  - **Lync / Skype / WebEx**
    - When using Lync or other conference software, be thoughtful about what is presented and who the recipient(s) may be.
  - **Vocera**
    - Be aware of your surroundings and comply with Vocera policies.
Safeguarding ePHI

- The use of USB (flash, thumb, jump) drives, CD’s is discouraged if PHI is involved.
  - If, your job duties require you to distribute or store ePHI on any electronic media per policy you must:
    - Obtain approval from your Director, IT Security, and Compliance.
    - Encrypted and/or password protected.

- Laptop computers, and other mobile devices which are used to access ePHI should be encrypted.
Social Media and Recording PHI

- Using social media to share patient information is prohibited per policy. This includes media such as Facebook, Twitter, Instagram, etc.
- Texting of patient information is prohibited unless:
  - Using a MSHA approved secure texting methodology is used and;
  - Department leader has approved the operational process of texting.
- Photography or videoing of patients requires an IT approved secure solution and must have department head approval.
- The use of personal equipment including cellular phone cameras to photograph patients is prohibited per policy.

**Review P&P HR-200-117 Conduct of MSHA Using Social Media **
Phishing/Spear Phishing/Malware

- Phishing Emails
  - Phishing is the attempt to acquire sensitive information such as usernames and passwords.
  - More advanced types of these attacks are called “Spear-phishing”. Spear-phishing attacks can capture financial data, even credit card details, by masquerading as a trustworthy entity (CEO, CFO, COO, etc.) in emails and may also contain links to websites that are infected with various forms of malware, including ransomware.

- If you receive a suspicious email, do not click on any embedded link on this message and promptly report to IS Help Desk.
Steps to Avoid Ransomware

- Do not reply to or visit any websites within any unexpected e-mail (especially from an unfamiliar sender).
- Hold the pointer over any link to see the real website it is connected to before clicking on a link.
- Limit any web browsing and use to official business websites only.
- If the text within an e-mail requires or has pressure to conduct immediate action by the user, it is likely fraudulent.
- Never reset a password from an unsolicited e-mail link. If you receive an e-mail that tells you to do so, visit the known primary site directly.
- Never use the same password for your work and personal log-ins.
HIPAA Security Knowledge Check

You are working on a BIG project, for work or part of your college classwork, which involves reviewing PHI and creating a summary report of your findings. You reviewed the medical records at a MSHA facility and created a listing of patient visit dates, patient name, and the patient age. You will be completing your summary report over the weekend while you are visiting your parents. What steps do you need to take before taking the listing outside of the MSHA facility?

A. Email the list to your personal email address.
B. Save the list on your personal jump drive that you use for all your college assignments.
C. Submit your request to your MSHA Director or MSHA IS Help Desk.
D. None of the above since the information on the list is not PHI.
C. Submit your request to your MSHA Director or MSHA IS Help Desk.
Physical Safeguards

- **Facility Access and Control**: A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

- **Workstation and Device Security**: A covered entity must implement policies and procedures to:
  - Specify proper use of and access to workstations and electronic media.
  - Regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

- In general, these safeguards require MSHA to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
Physical Safeguards (continued)

- Measures, policies and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

- In general, these safeguards require MSHA to:
  - Implement policies and procedures to control access to systems and facilities housing electronic PHI.
  - Implement policies and procedures to insure facility security and appropriate functions of workstations.
  - Implement policies and procedures that govern controls for devices and media.
Protected Health Information (PHI) originals or copies should not be taken outside of the organizations without MSHA approval.

- This includes reports, lists, census, emails, excel and Word files, etc., that contain PHI.

PHI that is taken outside of any MSHA covered entity, as part of an approved and valid healthcare operational reason should follow the physical safeguards per MSHA policy on External Transport of Patient Information.

- Patient information (including screenshots that only contain a patient’s name) should **not** be used in presentations.

**Review P&P IM-900-009 External Transport of Patient Information**

**Review P&P IM-900-020 Removal of Medical Records**
HIPAA requires organizations to designate someone to oversee responsibility of HIPAA security compliance. At MSHA, the HIPAA Compliance Officer in Corporate Audit and Compliance Services is the designated HIPAA Security Officer.

A. True
B. False
Answer to the HIPAA Security Rule Knowledge Check

- HIPAA requires organizations to designate someone to oversee responsibility of HIPAA security compliance. At MSHA, the HIPAA Compliance Officer in Corporate Audit and Compliance Services is the designated HIPAA Security Officer.

A. True
Software and Vendor Services

The installation of software or hardware is prohibited without:

- Approval by MSHA IS Dept.
- Requests must be submitted per MSHA IT guidelines and are subject to approval criteria.
- New applications that will access, use, collect PHI or use the internet must go through the organization's review and approval process (i.e. ETAF) prior to initiating the purchase.

Utilization of a vendor to provide a software solution or staffing resource requires:

- Financial review/approval
- ETAF review and approval
- Contracts development and possibly a business associate agreement.
Business Associates

- The Security Rule contains many other requirements that MSHA, as a covered entity, must meet to comply with HIPAA. These topics are briefly reviewed below:
  - **Business Associate Agreement (BAA):** Under certain conditions, MSHA is required to maintain legal contract (i.e. BAA) with business partners whose activity may involve the use, or disclosure of individually identifiable health information, in addition to an agreement/contract.
  - MSHA HIPAA Compliance Officer and Contracts Management Department should be consulted regarding contracts when patient information is involved.
Reporting Security Incidents or Concerns

- Report loss of any MSHA owned or managed device.
- Report loss of any personal device which may contain *any* patient information.
- **Immediately** notify MSHA IS Help Desk or MSHA Corporate Audit and Compliance Services Dept (CACS).
- Examples of devices that may contain PHI are:
  - Computers (laptop’s, netbooks, iPads, desktop, etc..)
  - CD’s, USB flash drive, thumb drive, jump drive
  - Hard drive
  - Cell phones used for work

**Review P&P IM-900-026 Reporting Potential or Actual Breaches of Patient Protected Health Information**
HIPAA Security Knowledge Check

You are the nurse currently assigned to an admitted patient. The patient’s attending physician sends you an email requesting that you send reply back via email with the patient’s lab results when the results are available. When the lab results are available you start to reply to the physicians email and notice that the email address for the physicians is not a MSHA email address. What should you do?

A. Page or call the physician with notification that you cannot send the lab results via email as it would be a policy violation.

B. Enter [securemail] in the beginning of the subject line of the email per policy.

C. Reply to the physician email and send the patient lab results via email.
B. Enter [securemail] in the beginning of the subject line of the email per policy.

**Refer to Policy IM-900-008 Electronic Mail Communication **
Workforce Member Responsibility

- The federal government requires that MSHA have policies to address disciplinary actions for team members who fail to comply with HIPAA Rules.
- Disciplinary action up to and including termination can occur for violation HIPAA Rules and/or organization policies.
- MSHA workforce members are responsible for protecting and securing PHI.
- Workforce members can be individually liable for HIPAA breaches.
- Report HIPAA Compliance concerns to MSHA ALERTLINE, or contact the HIPAA Compliance Officer.
Summary

- This course has provided an abbreviated overview of HIPAA:
  - Privacy Rules
  - Security Rules
  - Principles practiced throughout MSHA
- HIPAA policy and procedure available online in policy manager.
Who to Contact?

- HIPAA Security Officer: Donna Coomes
  - Telephone #: 423-302-3401
- MSHA Alert line 1-800-535-9057
- Discuss HIPAA concerns:
  - Your Director or Manager; or
  - Submit online using:
    - Patient Safety
    - Guest Feedback Reporting System
    - Email to CACSPrivacySecurity@msha.com
Almost finished....

Please close this window and return to TEDS to complete the test for this course.