Health Insurance Portability and Accountability Act

“HIPAA” Security

Health Insurance Portability and Accountability Act

“HIPAA” Security

Learning Objectives

- The purpose of this course is to increase your awareness of HIPAA security guidelines which are in place to protect the privacy of Protected Health Information and prevent security breaches
- By the end of this course, you should be able to:
  - Explain confidentiality, integrity, and availability as it relates to ePHI
  - Apply information safeguards
  - Identify your responsibilities under the HIPAA rule related to security
  - Understand how to report security concerns (i.e. complaints, incidents, violations and Breaches)

Privacy vs. Security

- **Privacy**
  - The Privacy Rule limits the Use and Disclosure of information that could potentially associate a Member's identity with his or her health information
  - MedTech Enginuity Corp. may not Use or Disclose Protected Health Information (PHI) except as authorized by the Member, or as permitted or required by law
- **Security**
  - The Security Rule requires MedTEC to implement administrative, technical and physical safeguards to insure the *confidentiality, integrity* and *availability* of PHI that is maintained in an electronic form referred to as ePHI
  - We must also protect ePHI against any reasonably anticipated related threats or hazards, and *unauthorized* Uses or Disclosures
  - This rule requires protection of MedTech Enginuity Corp./MedTEC information systems during processing and transmission of ePHI

Privacy vs. Security

- **Privacy**
  - The Privacy Rule limits the Use and Disclosure of information that could potentially associate a Member's identity with his or her health information
  - MedTech Enginuity Corp. may not Use or Disclose Protected Health Information (PHI) except as authorized by the Member, or as permitted or required by law
- **Security**
  - The Security Rule requires MedTEC to implement administrative, technical and physical safeguards to insure the *confidentiality, integrity* and *availability* of PHI that is maintained in an electronic form referred to as ePHI
  - We must also protect ePHI against any reasonably anticipated related threats or hazards, and *unauthorized* Uses or Disclosures
  - This rule requires protection of MedTech Enginuity Corp./MedTEC information systems during processing and transmission of ePHI

What is ePHI?

- Electronic Protected Health Information (ePHI) is Protected Health Information (PHI) that is:
  - transmitted by electronic media or
  - maintained in electronic media

What is ePHI?

- Electronic Protected Health Information (ePHI) is Protected Health Information (PHI) that is:
  - transmitted by electronic media or
  - maintained in electronic media

HIPAA Information Security

- It is important that all HIPAA related information be secure to insure *confidentiality, integrity and availability*
  - Confidentiality
    - Prevent unauthorized access or release of ePHI
    - Prevent abuse of access (identity theft, gossip)
  - Integrity
    - Prevent unauthorized changes to ePHI
  - Availability
    - Prevent service disruptions due to malicious or accidental actions, or natural disasters

HIPAA Information Security

- It is important that all HIPAA related information be secure to insure *confidentiality, integrity and availability*
  - Confidentiality
    - Prevent unauthorized access or release of ePHI
    - Prevent abuse of access (identity theft, gossip)
  - Integrity
    - Prevent unauthorized changes to ePHI
  - Availability
    - Prevent service disruptions due to malicious or accidental actions, or natural disasters

How Do We Protect ePHI?

- Develop, maintain and educate workforce members on MedTech Enginuity Corp./MedTEC HIPAA policies and procedures
- Infrastructure security
  - Computer network and systems security
  - Physical security
  - Workforce security
  - Backup and disaster recovery
  - Authentication and termination
  - Authorization and audit logs
- Responsibilities
  - User responsibility
  - Manager responsibility
  - Asset owner responsibility

How Do We Protect ePHI?

- Develop, maintain and educate workforce members on MedTech Enginuity Corp./MedTEC HIPAA policies and procedures
- Infrastructure security
  - Computer network and systems security
  - Physical security
  - Workforce security
  - Backup and disaster recovery
  - Authentication and termination
  - Authorization and audit logs
- Responsibilities
  - User responsibility
  - Manager responsibility
  - Asset owner responsibility

Regulation Specification

- Key *safeguards* are required to be in place to protect ePHI:
  - **Administrative Safeguards**
    - Policies and procedures
    - Responsibility
    - Awareness and training
    - Incident processing, sanctions
  - **Physical Safeguards**
    - Workstation use and security
    - Facility access control
    - Device and media control
  - **Technical Safeguards**
    - Access control
    - Audit control
    - Encryption and integrity control

Regulation Specification

- Key *safeguards* are required to be in place to protect ePHI:
  - **Administrative Safeguards**
    - Policies and procedures
    - Responsibility
    - Awareness and training
    - Incident processing, sanctions
  - **Physical Safeguards**
    - Workstation use and security
    - Facility access control
    - Device and media control
  - **Technical Safeguards**
    - Access control
    - Audit control
    - Encryption and integrity control

Consequences of Security Failures

- There can be multiple consequences for breaching security:
  - Member safety/medical care is compromised
  - Negative publicity
  - Increased costs
  - Identity theft
  - Members can become targets of con artists
  - Legal liability/lawsuits

Consequences of Security Failures

- There can be multiple consequences for breaching security:
  - Member safety/medical care is compromised
  - Negative publicity
  - Increased costs
  - Identity theft
  - Members can become targets of con artists
  - Legal liability/lawsuits

Types of Security Failures

- As much as we try to secure ePHI, security failures can happen

- Intentional attacks could include, but are not limited to:
  - Malicious software (Bots, Spyware)
  - Stolen passwords (Keyloggers)
  - Impostors calling or e-mailing to steal information (Phishing)
  - Theft (laptop, PDA)
  - Abuse of privilege (employee/VIP clinical data)

Types of Security Failures

- As much as we try to secure ePHI, security failures can happen

- Intentional attacks could include, but are not limited to:
  - Malicious software (Bots, Spyware)
  - Stolen passwords (Keyloggers)
  - Impostors calling or e-mailing to steal information (Phishing)
  - Theft (laptop, PDA)
  - Abuse of privilege (employee/VIP clinical data)

Types of Security Failures (continued)

- Employee Carelessness
  - Sharing passwords or User ID's
  - Not signing off the systems
  - Downloading and executing software
  - Sending ePHI outside MedTech Enginuity Corp./MedTEC without encryption
  - Not protecting PDA and laptop with password and encryption
  - Pursuing risky behavior – Improper web surfing and instant messaging
  - Not questioning or reporting suspicious or improper behavior

Types of Security Failures (continued)

- Employee Carelessness
  - Sharing passwords or User ID's
  - Not signing off the systems
  - Downloading and executing software
  - Sending ePHI outside MedTech Enginuity Corp./MedTEC without encryption
  - Not protecting PDA and laptop with password and encryption
  - Pursuing risky behavior – Improper web surfing and instant messaging
  - Not questioning or reporting suspicious or improper behavior

How Do We Protect Against Failures?

- Install anti-virus, anti-spyware solutions, install security patches and update daily
- Use caution when viewing web pages, e-mail attachments and programs
- Choose strong passwords, refuse to share it and change if you suspect a Breach
- Protect your laptop or PDA with a password
- Encryption on sensitive folders
- Do not allow copying to external storage devices such as CD, USB storage devices, etc.
- Do not abuse access privilege, report if you observe an abuse (if necessary, anonymously)
- Store ePHI carefully

How Do We Protect Against Failures?

- Install anti-virus, anti-spyware solutions, install security patches and update daily
- Use caution when viewing web pages, e-mail attachments and programs
- Choose strong passwords, refuse to share it and change if you suspect a Breach
- Protect your laptop or PDA with a password
- Encryption on sensitive folders
- Do not allow copying to external storage devices such as CD, USB storage devices, etc.
- Do not abuse access privilege, report if you observe an abuse (if necessary, anonymously)
- Store ePHI carefully

How Do We Protect Against Failures?

- Do not be responsible for another workforce member's abuse by neglecting to sign off
  - this negligence may lead to your suspension and termination
- Do not copy, duplicate or move ePHI without a proper authorization
- Do not email ePHI without encryption to addresses outside of the company.
  - **Internal:** Internal Email does not need to be encrypted as it remains within our Exchange server
  - **External:** MedTEC's email system has automatic ePHI detection in place and secure connections with our major vendors and partners. However, if you want 100% assurance that your email is delivered with encryption, you can include the keyword SECURE in the subject line
- Strictly follow MedTEC's policy of "Minimum Necessary" and "Need-to-Know"

How Do We Protect Against Failures?

- Do not be responsible for another workforce member's abuse by neglecting to sign off
  - this negligence may lead to your suspension and termination
- Do not copy, duplicate or move ePHI without a proper authorization
- Do not email ePHI without encryption to addresses outside of the company.
  - **Internal:** Internal Email does not need to be encrypted as it remains within our Exchange server
  - **External:** MedTEC's email system has automatic ePHI detection in place and secure connections with our major vendors and partners. However, if you want 100% assurance that your email is delivered with encryption, you can include the keyword SECURE in the subject line
- Strictly follow MedTEC's policy of "Minimum Necessary" and "Need-to-Know"

Combat the Threat

- You can help safeguard information:
  - Lock or log off of the computer system before you walk away
  - Re-position computer monitors so passers-by cannot view the information
  - Do not share passwords or User ID's
  - Wear your picture ID badge at all times

Combat the Threat

- You can help safeguard information:
  - Lock or log off of the computer system before you walk away
  - Re-position computer monitors so passers-by cannot view the information
  - Do not share passwords or User ID's
  - Wear your picture ID badge at all times

Rules for Secure Password Management

- It is important that you have a secure password
  - NEVER tell or share your password with anyone
  - Avoid maintaining a paper record of password(s), unless record can be stored securely
    - Do Not post your password(s) in or around your workstation
    - Do Not use POST-IT notes listing password(s)
    - Do Not document and save your password(s) in clear text saved to a shared drive or site
    - Electronically store password(s) in encrypted form with approved application such as KeePass Password Safe or save in a file with password protection
    - Do not include password(s) in any automated log-on process
  - Create a password that is hard to guess following established guidelines
  - If you think someone has learned your password, notify IT-Support and change it immediately

Rules for Secure Password Management

- It is important that you have a secure password
  - NEVER tell or share your password with anyone
  - Avoid maintaining a paper record of password(s), unless record can be stored securely
    - Do Not post your password(s) in or around your workstation
    - Do Not use POST-IT notes listing password(s)
    - Do Not document and save your password(s) in clear text saved to a shared drive or site
    - Electronically store password(s) in encrypted form with approved application such as KeePass Password Safe or save in a file with password protection
    - Do not include password(s) in any automated log-on process
  - Create a password that is hard to guess following established guidelines
  - If you think someone has learned your password, notify IT-Support and change it immediately

Password Management Guidelines

- Length and Complexity:
  - The minimum length of passwords shall be set as 7 characters
- Composition:
  - Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example:!, @, #, $, %)
      - A new password should contain at least 3 characters that are different than those found in the old password which it is replacing.
  - Use as many characters as possible (the longer the password, the harder it is to crack)
  - Not be the same or similar to the last 10 used passwords

Examples of How to Create a Strong Password

1. **Mix upper and lowercase characters**
   - 3bLINdmice
   - 5gOLDenrings
   - 4cALLingbirdS

2. **Replace letters with numbers**
   - Replace “E” with “3”
     - “Sp3cial” or “3l3gant”

. **Combine two words by using a special character**
   - Roof^Top
   - Sugar$Daddy
   - B@tterup!

4. **Use the first letter from each word of a phrase from a song**

   “Oops! I did it again” becomes “O!idia”

Use a Strong Password

- To protect your password from password decoder programs use strong passwords which:
  - Based on something that can be easily guessed or obtained using personal information (e.g. names, favorite sports team, etc.)
  - Based on users personal information or that of his or her friends, family members, or pets (e.g. logon I.D., name, birthday, address, phone number, social security number)
  - Words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon
  - Based on publicly known fictional characters from books, films
  - Based on the company's name or geographic location or application name

Use a Strong Password

- To protect your password from password decoder programs use strong passwords which:
  - Based on something that can be easily guessed or obtained using personal information (e.g. names, favorite sports team, etc.)
  - Based on users personal information or that of his or her friends, family members, or pets (e.g. logon I.D., name, birthday, address, phone number, social security number)
  - Words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon
  - Based on publicly known fictional characters from books, films
  - Based on the company's name or geographic location or application name

Think Before You Click

- Sometime spam emails are hard to decipher
- Delete suspect emails without opening them, such as those from unknown users with attachments
- Turn off the preview pane in your email application because this will automatically open an email when you click on it and could infect your computer
- Never forward emails that you think may be infected with a virus
- Do not open email attachments that end in .vbs,.exe, .com, .shs, .bat, .cmd, .inf, .sct, .vbe, .vb, .wsc, .wsf or .wsh
  - Files that end with an ".exe" are executable files, or software programs. Viruses or malicious software programs are often contained in downloaded executable files.
  - These types of attachments can contain viruses or launch viruses into your system

Think Before You Click

- Sometime spam emails are hard to decipher
- Delete suspect emails without opening them, such as those from unknown users with attachments
- Turn off the preview pane in your email application because this will automatically open an email when you click on it and could infect your computer
- Never forward emails that you think may be infected with a virus
- Do not open email attachments that end in .vbs,.exe, .com, .shs, .bat, .cmd, .inf, .sct, .vbe, .vb, .wsc, .wsf or .wsh
  - Files that end with an ".exe" are executable files, or software programs. Viruses or malicious software programs are often contained in downloaded executable files.
  - These types of attachments can contain viruses or launch viruses into your system

How do we protect against Malicious

- Antivirus software is installed by Information Technology (IT) and kept up-to-date
- Do not:
  - Bypass or disable anti-virus software
  - Modify web browser security settings
  - Install unauthorized software
    - Use only IT department installed software
- Immediately report incidents of suspected or known malicious software to your supervisor and the IT Department
- Call IT Support at 301.352.0344

How do we protect against Malicious

- Antivirus software is installed by Information Technology (IT) and kept up-to-date
- Do not:
  - Bypass or disable anti-virus software
  - Modify web browser security settings
  - Install unauthorized software
    - Use only IT department installed software
- Immediately report incidents of suspected or known malicious software to your supervisor and the IT Department
- Call IT Support at 301.352.0344

Security Scenario - Question

- HIPAA's Security Rule calls for alerting computer users to signs of malicious software or misuse of your computer or your account, and reporting them. Which of the following might be such a sign?
  - You try to log on, and the system rejects your password, but you're sure you typed it correctly
  - You log on, and your usual screen has changed
  - You log on and see a welcome message stating that you last logged in on Friday, but that's impossible since you were on vacation
  - Your computer runs at a crawl and sometimes freezes and it never did this before
  - Any of the above might be a sign of malware or an indication that someone has used your access

Security Scenario - Answer

- All of the above
- You would:
  - Immediately report incident of suspected or known malicious software to your supervisor and the IT Department
  - Call IT Support at 301.352.0344

Storage and Backup

- What is your responsibility as a user in ***storing*** ePHI to keep it safe and insure it is backed up?
  - You should save ePHI data to the appropriate drive and in the appropriate manner on the file server so the data is ***backed up*** regularly
  - **DO NOT** save data containing ePHI such as patient or provider records, lists of providers and client information with SSN's, password cheat sheets, etc., to the corporate file shares unless documents are *password protected* or a *User group* is established *restricting access*
  - **DO NOT** save ePHI data to your computer hard drive (C: drive) or removable storage media (i.e. USB, CD, DVD)

HIPAA Security Requirements for Building Access

- Immediately report lost/stolen cards or keys
- Wear your picture ID badge at all times
- Make sure visitors sign in and are escorted to destination

HIPAA Security Requirements for Building Access

- Immediately report lost/stolen cards or keys
- Wear your picture ID badge at all times
- Make sure visitors sign in and are escorted to destination

HIPAA Security Requirements for Workstation

- Properly safeguarding each workstation computer is one of the most important ways to protect data from corruption or loss:
  - Log off when you are done working on your computer
  - Lock your computer session when it is left unattended
  - Protect ePHI from unauthorized access if you work from home
  - Laptops should be locked up when you are out of the office and should be secured at all times when traveling
- Clear workstation and working areas before leaving the office premises even during a break
  - If possible, position your computer monitor so that data shown on screen is not visible to those who walk by
- Do not relocate any computer equipment without IT approval

HIPAA Security Requirements for Workstation

- Properly safeguarding each workstation computer is one of the most important ways to protect data from corruption or loss:
  - Log off when you are done working on your computer
  - Lock your computer session when it is left unattended
  - Protect ePHI from unauthorized access if you work from home
  - Laptops should be locked up when you are out of the office and should be secured at all times when traveling
- Clear workstation and working areas before leaving the office premises even during a break
  - If possible, position your computer monitor so that data shown on screen is not visible to those who walk by
- Do not relocate any computer equipment without IT approval

How to Lock Your Computer Session

- Lock your computer session when leaving your computer unattended by:
  - Press Ctrl+Alt+Delete keys to Log Off or Lock Workstation
  - Use the Windows key + L to Lock Workstation

- Locking your computer session when you leave your computer unattended does not shut down any document or program you have open
  - It is a key to good security and should always be practiced
  - Locking your computer session prevents unauthorized use

How to Lock Your Computer Session

- Lock your computer session when leaving your computer unattended by:
  - Press Ctrl+Alt+Delete keys to Log Off or Lock Workstation
  - Use the Windows key + L to Lock Workstation

- Locking your computer session when you leave your computer unattended does not shut down any document or program you have open
  - It is a key to good security and should always be practiced
  - Locking your computer session prevents unauthorized use

What is Company's Responsibility?

- It is the company's responsibility to safeguard provider records that include patient names, dates of birth and social security numbers and any other information that could identify the patient by protecting our information infrastructure

- A security Breach of privacy could not only damage our reputation and hurt an individual employee or provider, it could also lead to fines, civil or criminal liability and even jail time

What is Company's Responsibility?

- It is the company's responsibility to safeguard provider records that include patient names, dates of birth and social security numbers and any other information that could identify the patient by protecting our information infrastructure

- A security Breach of privacy could not only damage our reputation and hurt an individual employee or provider, it could also lead to fines, civil or criminal liability and even jail time

PDAs, laptops, and portable media

- Many healthcare workers use PDAs and laptops, and the most frequent risk when using these devices is the risk of theft. This may result in a loss of equipment and potential loss of data confidentiality. PDAs, laptops and any portable media should be locked in a drawer or briefcase when not in use.
  - If your device is lost or stolen, notify your supervisor and/or the Privacy Official immediately
- The following are helpful tips to keep ePHI secure when using a PDA, laptop, tablet or other portable media:
  - Do not save PHI on a portable device unless it is protected by a password
  - Do not keep passwords and access codes on your PDA under any circumstances
  - Work with the IT Support to insure and protect back-ups from your portable device
  - **Employees should not have ePHI saved on laptops**

Security Scenario - Question

- It has been the practice to leave the email system open and logged on for easy access. This allows workforce members to remain continuously logged onto the computer to review emails quickly.

- Is this an appropriate practice under HIPAA?

Security Scenario - Question

- It has been the practice to leave the email system open and logged on for easy access. This allows workforce members to remain continuously logged onto the computer to review emails quickly.

- Is this an appropriate practice under HIPAA?

Security Scenario - Answer

- No
- It may seem like a timesaver but this practice is equivalent to sharing a password
- When others are allowed to access under your password, there can be no way to audit who and when records are accessed

Security Scenario - Answer

- No
- It may seem like a timesaver but this practice is equivalent to sharing a password
- When others are allowed to access under your password, there can be no way to audit who and when records are accessed

Maintaining Records and HIPAA Security

- Safeguard information that is in your possession
- Do not leave information unattended
- Secure medical records and any other hard copy PHI
- Log off of computer systems after accessing electronic data
- Do not leave information visible or an unattended computer monitor or fax tray
- Shred sensitive paper data

Maintaining Records and HIPAA Security

- Safeguard information that is in your possession
- Do not leave information unattended
- Secure medical records and any other hard copy PHI
- Log off of computer systems after accessing electronic data
- Do not leave information visible or an unattended computer monitor or fax tray
- Shred sensitive paper data

HIPAA Summary

- The Security Rule requires MedTEC to:
  - insure the confidentiality, integrity, and availability of all electronic PHI that it creates, maintains, receives, or transmits;
  - protect against any reasonable anticipated threats or hazards to the security and integrity of such information;
  - protect against inappropriate uses and disclosures;
  - insure workforce compliance with standards (training)

HIPAA Summary

- The Security Rule requires MedTEC to:
  - insure the confidentiality, integrity, and availability of all electronic PHI that it creates, maintains, receives, or transmits;
  - protect against any reasonable anticipated threats or hazards to the security and integrity of such information;
  - protect against inappropriate uses and disclosures;
  - insure workforce compliance with standards (training)

HIPAA Summary

- Be sure you know who your Privacy and Security Officials are, and how to contact them
- Be sure to ask if you're not sure what's the "right" thing to do
- It is part of your job to report instances in which you suspect our privacy or security policies or practices are being violated

Reporting

- Be sure to immediately report any suspected privacy or security incident, violation or Breach such as:
  - Unauthorized or suspicious visitors
  - Logged on but unattended workstations
  - Uncontrolled access to areas that house equipment and/or PHI
  - Passwords on Post-it™ notes
  - Workforce members accessing records without a “Need to Know”

Completion

Congratulations!
You have now completed
the
HIPAA Security Training course.

Completion

Congratulations!
You have now completed
the
HIPAA Security Training course.