DynPro

HIPAA Security Awareness & Training

What You Need To Know

Training Overview

This course will discuss the following subject areas:

- How this training relates to you
- Overview of the HIPAA (Health Insurance Portability and Accountability Act) Security rule and terms you should know
- Three areas that HIPAA Security regulations indicate are critical in maintaining the security of electronic Protected Health Information (e-PHI).
  - Minimizing the introduction of malicious computer software
  - Proper use of system User IDs
  - Creating and maintaining robust passwords
- Special responsibilities for laptop users
- HIPAA Security sanction policy

Purpose and Content

Why is HIPAA Security Awareness training mandatory?

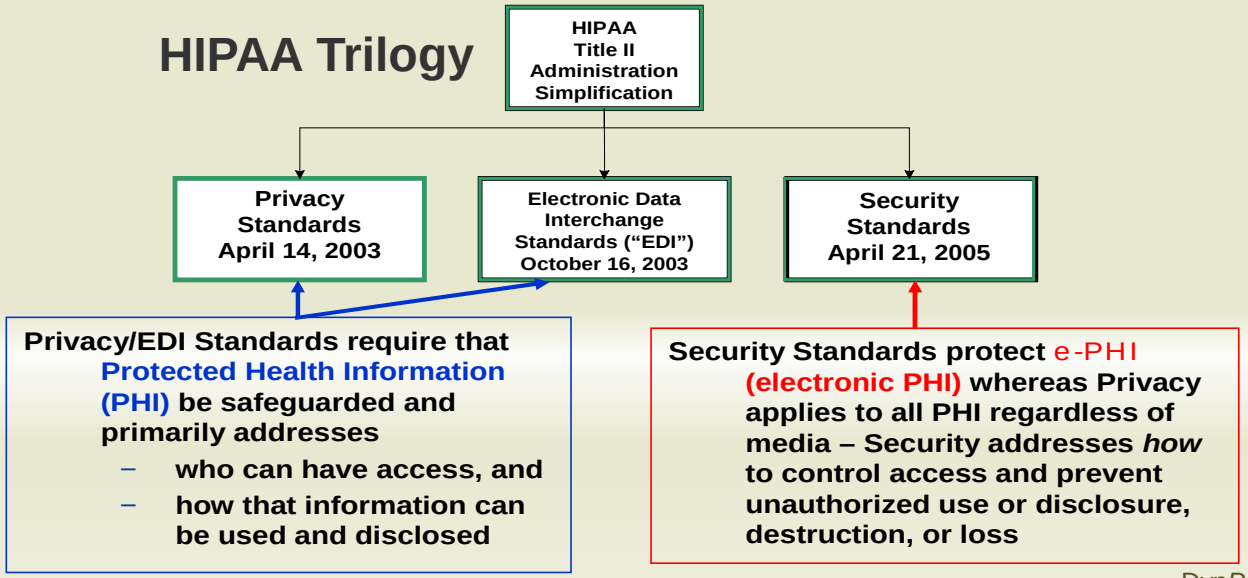
Because you are an employee who has access to computer equipment or software containing protected health information related to the Client e-PHI data, the HIPAA Security rule requires that you participate in the HIPAA Security awareness training to learn about the basic procedures you must follow to protect that information. Following our electronic security procedures is important because the procedures help to protect the information's:

- ***Confidentiality*** (only the right people see it)
- ***Integrity*** (the information is what it is supposed to be – there has been no unauthorized alteration or destruction.
- ***Availability*** (the right people can see it when needed)

Terms You Should Know

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)

✓ Title II of the HIPAA act, administrative simplification, defines three sets of standards



Terms You Should Know

- **HIPAA Covered Entity and Business Associate is:**

✓ A HIPAA covered entity is a health care provider, health plan, or health care clearinghouse

✓ Covered entities must comply with the standards set in the HIPAA rules

✓ DynPro® is a business associate because it does not sponsor self-insured plans, assists with plan administration, or stores medical and any confidential data

- **Protected Health Information (PHI) is:**

✓ Individually identifiable health information

✓ About an individual's past, present, or future physical or mental health or condition; or

✓ About an individual's past, present, or future provision of or payment for health care; and

✓ Created or received in any medium (verbal, written, or electronic) by a HIPAA covered entity

Terms You Should Know

- **The HIPAA privacy rule sets standards for safeguarding of all forms of PHI, including e-PHI.**

- **Electronic PHI (e-PHI) is:**

✓ Electronically created,

✓ Electronically received,

✓ “At rest” or maintained in a storage device such as a computer hard drive, disk, CD, tape, or

✓ “In transit” via the Internet, dial-up lines, etc. For example, e-mail, Secure File Transfer Protocol (SFTP), Electronic Data Interchange (EDI), Interactive Voice Response (IVR), and fax-back systems used to transmit PHI.

Terms You Should Know

- **Electronic PHI (e-PHI) is *not*:**

✓ PHI that was not in electronic form before transmission, such as information shared by: person-to-person telephone calls, copy machines, paper-to-paper fax machines, voicemail, or de-identified information

- The HIPAA Security rule establishes standards for safeguarding e-PHI only.

Objectives of the HIPAA Security Rule

- Secure e-PHI “at rest,” while in the custody of group health plans
- Secure e-PHI “in transit,” both between health plans and from a health plan to a third party
- Protect against reasonably anticipated:
  - Threats or hazards to e-PHI security or integrity
  - Unauthorized uses or disclosures
- Requires group health plans to:
  - Perform a risk analysis
  - Remedy security deficiencies
  - Document policies and procedures
  - Train personnel
  - Monitor ongoing compliance efforts
  - Enforce sanction policy

Objectives of the HIPAA Security Rule

- Procedures implemented to comply with the HIPAA Security rule must be reviewed and modified, as needed, to ensure the reasonable and appropriate protection of e-PHI over time

- HIPAA Security compliance is an on-going effort that must be constantly monitored

DynPro

Critical Security Risks

Critical Security Risks

- Three critical security risks must be eliminated or minimized by all DynPro® staff to ensure the confidentiality, availability, and integrity of e-PHI:

  1. **Malicious computer software, such as viruses**
  2. **Unauthorized use of system user IDs**
  3. **Weak or unprotected system and file passwords**

Malicious Software

- Malicious software is:
  - Software designed to damage or disrupt a system
  - Software that has an intentional negative impact on the confidentiality, availability, or integrity of PHI

- Malicious software can:
  - Destroy your computer files, or
  - Block your access to critical computer applications

- Malicious software includes: “viruses," “worms," and “trojan horses”

Malicious Software:
Computer Viruses

- A computer virus is:
  - A program or application loaded onto a computer without your knowledge, permission, or desire
  - Performs malicious actions, such as using up computer resources or destroying your files
  - Works by attaching itself to another legitimate or authorized program

Malicious Software:
Computer Worms

- A computer worm is:
  - A special type of virus
  - A self-contained program that works *without* having to attach to a legitimate/authorized program
  - Causes harm by using up system disk space and memory, depriving legitimate/authorized programs
  - Commonly noticed only when uncontrolled replication slows or halts other tasks

Malicious Software:
Trojan Horses

- A trojan horse:
  - Masquerades as a harmless, helpful application
    - In reality, it hides inside another program and performs an unintended or malicious function
  - A trojan horse can be just as destructive as a virus
    - It remains in the computer and either damages it directly or allows someone at a remote site to control it
  - The worst type of trojan horse claims to rid your computer of viruses but instead introduces viruses onto your computer

Malicious Software:
How Does It Get On My Computer?

- Infected email attachments
- Computer software from non-secure sources
  - Websites
  - Unlicensed software
- Files stored on external electronic storage media
  - Diskettes, Portable Data Storage Devices or CDs could contain malicious software

Malicious Software:
How Can I Keep It Off My Computer?

- ***Be suspicious!*** Don't open e-mails or e-mail attachments that are from suspicious or unknown sources or have suspicious subjects
- ***Report suspicious e-mail*** to the DynPro® Help Desk
- ***Comply*** with DynPro® instructions to ensure your workstation virus protection software is kept up-to-date.

Malicious Software:
How Can I Keep It Off My Computer?

- ***Never*** copy, download, or install computer software without permission;
- ***Never*** disable or tamper with the virus protection software installed on your workstation and/or laptop
- ***Always scan*** files from external storage media before copying them to detect the presence of malicious software
  - The virus protection software installed on your workstation or laptop automatically scans files being transferred to or copied from external storage media
- ***Make sure*** your home workstation or laptop has up to date virus protection software

Question #1
Malicious Software

- How often should the computer virus software on my workstation or laptop be updated?

  A. Never; once installed, it never needs to be updated

  B. As soon as the updates are available

  C. Only after a security incident related to malicious software has occurred

Question #1
Answer

- **The correct answer is B!**
  Computer virus protection software should be kept as up-to-date as possible in order to ensure that the appropriate safeguards are in place to protect against the new and ever changing malicious software threats that are present.

Malicious Software

How DynPro® Safeguards Against Malicious Software

- Workstations, laptops and servers have virus protection software to detect and help eliminate malicious software

- The name of the current virus protection software that DynPro® employs is **Symantec Anti-Virus.**

Malicious Software
Your Responsibilities

- Do not open suspicious e-mails or e-mail attachments
  - Report suspicious e-mail to the DynPro® Help Desk
- Keep your workstation virus protection software up to date
- Always read security alerts released by software vendors
- Never copy, download, or install unfamiliar computer software
- Never disable or tamper with the virus protection software installed on your workstation and/or laptop
- Always scan files from external storage media before copying them to detect the presence of malicious software
- Make sure your home workstation or laptop has up-to-date virus protection software installed on it

Malicious Software

Reporting Security Incidents

- Security incidents related to malicious software should be reported to the DynPro® ' Help Desk
- In addition, DynPro® employees and contractors who are aware of any misuse of company equipment, software or data within the agency must promptly notify the DynPro® Information Security Officer

Question #2

Reporting Security Incidents

- All suspected security incidents related to a malicious software attack should be reported to the DynPro® Help Desk as soon as possible.

  Is the above statement **True or False**?

Question #2
Answer

- The correct answer is **True**!

  In order to minimize the harm done by a malicious software attack it is critical that the DynPro® Help Desk is notified as soon as possible so that the appropriate corrective actions can be taken immediately.

Unauthorized Use

Passwords and/or User IDs

- Keeping your individual system user IDs and passwords **secret** is essential to maintain the confidentiality, availability, and integrity of PHI
  - By keeping your user ID and password confidential, you help ensure that PHI will be maintained correctly
  - Unauthorized use of individual user ID compromises PHI and defeats the audit trails designed to monitor PHI use
- User IDs for terminated personnel are disabled immediately

Never Share User IDs Or Passwords

- Sharing user IDs and passwords defeats the authorization procedures that have been put in place to control access to PHI based on a user's job responsibilities
- **You are Solely responsible for all actions taken with your user ID**

Never Leave A Written Clue…

Protect Your Password and User ID

- Do not leave information at your workstation, laptop or desk that could divulge what your system user ID and passwords are
  - Never leave any written record of your system user ID and passwords near your desk or workstation
- If you have to write them down, keep a record of passwords and system user IDs in a secure location *away from your desk* and/or workstation
  - Never keep a record of your system user ID or passwords in luggage or laptop bags if they are going to be out of your immediate control

Your Responsibilities

As a DynPro® Employee

- Never use another employee's user ID and password
- Never ask another employee to reveal his/her personal user ID and password
- Never reveal your user ID and password except:
  - To the appropriate **staff member** upon request, in order to resolve problems
- **You are responsible for controlling your password maintenance!**

Question #3
Test Yourself

- **Question**
  In case of emergency, it is a good practice to hide a copy of your user ID and password under your workstation keyboard at your desk.

  Is the above statement true or false?

Question #3
Answer

- **The correct answer is False**
  You should not leave information at your workstation, laptop or desk that could divulge your system user ID and password because it provides easy access to unauthorized persons. If you must keep a record of this information, store it in a secure location away from your desk and/or workstation. Never keep a record of your system user ID or password in luggage or laptop bags.

Weak or Ineffective Passwords

- Maintaining secure and strong passwords for systems and files is an essential element in achieving competent security for PHI
  - Passwords are your first line of defense for protecting the confidentiality and integrity of systems and files
  - Secure passwords are an essential safeguard against unauthorized use of your system user ID or unauthorized access to your files

- To be effective, passwords have to be:
  - **Private** and
  - **Difficult to discover**

What Makes a Password STRONG?

- It cannot easily be found out
  - **12345**, **abcde**, your **name**, **birthday**, or the **name of your cat** are **NOT** strong passwords!
- It typically contains **more than 8 characters**
- It contains of a **random combination of numbers**, **alphabetic characters**, and **special characters**
  - G25#V74ZHI is a good example of a strong password

Tips for STRONG Passwords

- Avoid proper names or personal initials
- Avoid real words contained in either English or foreign language dictionaries
- Avoid personal dates of significance, like birth dates or anniversaries
- Never use a repeating pattern of letters and/or numbers
- Never repeat the corresponding user ID as part of the password
- Always use a combination of letters, numbers and special characters, for example: **A9HZ?7YT**

File Protection Tips

- If you need to password protect a file, a strong file password is just as critical as strong system user ID
- Each file that needs protection should have its own unique password
  - Never use the same password for multiple files
- Don’t store the file’s password in the same location as the file itself
- If a password protected file is distributed via email, never include the password in the same email
- Give file passwords only to those people who need to access the data contained in those files
- Change the file password whenever changes occur in personnel who have been granted file access

Question #4
Test Yourself

- **Which of the following is a characteristic of a strong password?**

  A. Contains the employee's date of birth

  B. An easy to remember word out of the dictionary

  C. A sequential string of either letters or numbers

  D. Random letters, numbers, and punctuation marks

Question #4
Answer

- **The correct answer is D!**

- Robust passwords consist of a combination of letters, common numbers and special characters. Password consisting of eight characters with combination of letters, numbers and special characters are considered to be strong. Passwords comprised of repeating numbers, personal information (i.e., birth date), or common words may be easily guessed.

What Responsibility Do you Have As a Laptop User?

- Portable devices present greater risks because they can easily fall into the hands of unknown persons. These risks can be greatly reduced by your observing the following guidelines:
  - Keep portable devices that could provide access to e-PHI under careful control:
    - Keep these items in your personal possession when in public places (e.g., airports, restaurants).
    - Do not treat them as “checked baggage” (e.g., on trains, airplanes, etc.); keep them with you while traveling.
    - Place them into a locked suitcase when leaving them in a hotel room or other only semi-private location.
    - Exit all programs when the device is not in use.
  - Report immediately to ***Information Security*** if your device is missing or you believe an unauthorized use has been made of it.

DynPro

Security Policies and Procedures

Security Policies and Protection

Overview

- The HIPAA Security rule requires that DynPro® implement reasonable and appropriate policies and procedures to comply with the HIPAA Security standards, implementation specifications, or other requirements
- DynPro® may change its security policies and procedures at any time, if changes are documented and implemented in accordance with the HIPAA Security rule

Security Policies and Protection
Developing Procedures

- Security policies and procedures are developed to:
  - Identify and understand vulnerabilities
  - Implement procedures to protect e-PHI and respond to threatening activities
  - Correct any inappropriate activities
  - Understand what procedures to follow in a given situation, and how to apply them
  - Meet DynPro®'s technology needs

Security Procedures

Reviewing and Modifying Procedures

- The HIPAA Security rule requires DynPro® to implement policies and procedures
  - Policies and procedures must be reasonably designed and appropriate for the size and type of activities that relate to e-PHI
- Documentation must be in written (or electronic) form
- Any organizational or technological change may require updates to the security policies and procedures
- Regular, periodic reviews and updates of policies and procedures are also required

Security Alerts and Reminders

Why Read Them?

- **Security alerts** issued by DynPro® contain important information and instructions on how to safeguard against new sources of malicious software threats

- **Security reminders** contain important suggestions and methods of improving your ability:
  - To safeguard against malicious software threats, and
  - To maintain secure individual system user IDs and passwords

Policies Your Must Know and Comply With

- DynPro® has policies prohibiting both the sharing of individual system user IDs and passwords, and the misuse of DynPro® system software

Question #5
Test Yourself

- **If you receive a security reminder or security alert in your e-mail in box you should?**

A. Delete it without reading its contents

B. Immediately open the e-mail, read it, and follow all of the instructions

C. If you are busy, open and read it later

D. Follow the instructions but only if you think that they apply to you

Question #4
Answer

- **The correct answer is B!**
  The purpose of security reminders and alerts is to assist in preventing malicious software attacks. By paying immediate attention to the instructions contained in the security reminders and alerts the potential of a successful malicious software attack is greatly reduced.

Recap of Lessons Learned

- These security safeguards are essential to protect the confidentiality, integrity and availability of DynPro® systems and data, and must be followed by all workforce staff at all times:
  - Minimize and eliminate risks associated with malicious computer software
  - Safeguard against unauthorized use of system user IDs
  - Maintain secure and strong passwords for systems and files

HIPAA Security Sanction Policy

- DynPro® is committed to protecting the e-PHI in our control and that we maintain on behalf of our health plans. We will enforce disciplinary sanctions on those employees who violate the company-wide HIPAA Security policy and underlying procedures. Based on the facts and circumstances of a particular violation, sanctions may range from oral warnings to termination of employment.

Congratulations

- You have completed the HIPAA Security Awareness Training
- DynPro® appreciates your participation in the HIPAA Security awareness training and your efforts in maintaining the confidentiality, integrity and availability of e-PHI