# HIPAA

*PRESENTED BY*

## SHARON MOREHEAD



# Forms of Sensitive Information

- Sensitive information can exist in various forms…



**Printed**



**Spoken**



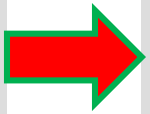
**Electronic**

**It is the responsibility of every employee to protect the privacy and security of sensitive information in ALL forms.**

# HIPAA Privacy and Security Rules

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect a subset of Sensitive Information known as Protected Health Information (PHI).
- In 2009, HIPAA was expanded and strengthened by the HITECH Act (Health Information Technology for Economic and Clinical Health). In January of 2013, the Department of Health and Human Services issued a final rule ("Final Rule") implementing HITECH's statutory amendments to HIPAA. The deadline for compliance was September 23, 2013.

This training module focuses on two primary HIPAA rules as amended by HITECH:



**Section 1. The HIPAA Privacy Rule**
**Section 2. The HIPAA Security Rule**

# HIPAA Privacy Rule Overview



# Covered Entities Have a Duty to Protect PHI

- A “covered entity” is any person or organization that furnishes, bills, or is paid for health care services in the normal course of business. Pursuant to HIPAA, individually identifiable health information collected or created by a covered entity is considered “protected health information,” or PHI. The APWU Health Plan is governed by HIPAA requirements.



# PHI Defined

- PHI is generally defined as any information that can be used to identify a patient, whether living or deceased, that relates to the patient's past, present, or future; physical or mental condition, including healthcare services provided and payment for those services.





# What is PHI?

## Identifiers include (but are not limited to):

- Name
- Geographic Information *(such as home or work address)*
- Social Security Number
- Medical ID Number
- Medical Record Number
- Insurance Beneficiary Numbers
- Account Numbers
- Photographic and Biometric Identifiers
- Date of Birth
- Date of Services
- Clinical Notes/Details
- Phone/Fax numbers
- Email address
- Medication Information

# Breaches

- A breach occurs when information that, by law, must be protected is:



  - lost, stolen or improperly disposed of (i.e. paper or device upon which the information is recorded cannot be accounted for);
  - "hacked" into by people or mechanized programs that are not authorized to have access (i.e., the system in which the information is located is compromised through a "worm"), or
  - communicated or sent to others who have no official need to receive it (i.e., sending member PHI to the wrong person or vendor).

# Penalties for Breaches

- Breaches of the HIPAA Privacy and Security Rules have serious ramifications for all involved. In addition to sanctions imposed by the APWU Health Plan, such breaches may result in civil and criminal penalties.



Statutory and regulatory penalties for breaches may include:

**Civil Penalties: $50,000** per incident up to $1.5 million per incident for violations that are not corrected, per calendar year.

**Criminal Penalties: $50,000 to $250,000** in fines and up to **10 years in prison**.

# Quick Review

- Sensitive information exists in many forms: printed, spoken, and electronic.
- There are a number of state and federal laws that impose privacy and security requirements, including HIPAA.
- Two primary HIPAA regulations are the **Privacy Rule** and the **Security Rule**.
- When used to identify a member and when combined with health information, HIPAA identifiers create PHI.
- An employee must have a member's **written authorization or a job-related reason for accessing** or disclosing member information.
- Breaches of information privacy and security may result in both **civil and criminal penalties**, as well as APWU Health Plan sanctions. **Employees must report such breaches.**

# Member Rights

- HIPAA sets forth the following individual rights for patients:
  - To receive a copy of the Health Plan's Notice of Privacy Practices
  - To appoint a Personal Representative
  - To request restrictions and confidential communications of their PHI
  - To inspect and/or receive an electronic copy of their healthcare records




  - To request corrections of their healthcare records
  - To obtain an accounting of disclosures (i.e., a list showing when and with whom their information has been shared)
  - To file a complaint with a healthcare provider or insurer and the U.S. Government if the patient believes his or her rights have been denied or that PHI is not being protected
  - To receive notice of a breach of their unsecured PHI

# Privacy Notice Contains

- The Privacy Notice tells the member:
  - How the Health Plan will use and share their PHI;
  - Informs members of their individual rights;
  - The Health Plan's responsibilities in protecting their PHI;
  - The title and contact information for the Privacy Specialist;
  - The process for filing complaints or requesting copies of their records.



# Distributing the Privacy Notice

- Who gets it, when and how?
  - Every new member gets a copy in their enrollment kit
  - If there is a significant change, we post it on our website: **www.apwuhp.com**
  - Provide a printed copy when requested



# Disclosures of PHI

- HIPAA Regulations **permit** use/disclosure of PHI for:
  - Providing medical treatment
  - Processing healthcare payments
  - Conducting healthcare business operations
  - Public health purposes as required by law
- The Health Plan **may not** otherwise access or disclose PHI unless:
  - The member has given written permission
  - Proper procedures are followed for using data in research
  - Required or permitted by law




**Note:** The Final Rule now protects the PHI of a **deceased individual** for period of **50 years following the death** of that individual.

# Business Associates Defined

- An outside company or individual is a Business Associate of the Health Plan when performing functions or providing services involving the use or disclosure of PHI maintained by the Health Plan.
- Under the Final Rule, a Business Associate is **directly liable for compliance** with HIPAA Privacy and Security requirements and must:
  - enter into a Business Associate Agreement (called a BAA) with the covered entity (APWU Health Plan);
  - use appropriate safeguards to prevent the access, use or disclosure of PHI other than as permitted by the contract, or BAA, with the covered entity;
  - obtain satisfactory assurances from any subcontractor that appropriate safeguards are in place to prevent the access, use or disclosure of PHI entrusted to it;
  - notify the covered entity of any breach of unsecured PHI for which the Business Associate was responsible upon discovery;
  - ensure its employees and/or those of its subcontractors receive HIPAA training; and
  - protect PHI to the same degree as a covered entity.

# Quick Review

- Under HIPAA, members have the right to:
  - Receive a copy of APWU Health Plan's Notice of Privacy Practices;
  - Receive an electronic copy of their healthcare records ;
  - Ask for corrections to their healthcare records;
  - Receive an accounting of when and to whom their PHI has been shared;
  - Restrict how their PHI is used and shared;
  - Authorize confidential communications of their PHI to others;
  - Receive notice of a breach of their unsecured PHI;
  - File a HIPAA complaint;
  - APWU Health Plan may use or share only the minimum necessary information to perform its duties;

# Quick Review *(continued)*

- Members must sign a Personal Representative Form, or an Authorization to Release PHI Form, before the Health Plan can release their PHI to a third party not involved in providing healthcare;
- A researcher or healthcare provider is not entitled to use PHI in research without the appropriate HIPAA authorization or a waiver of authorization;
- A contractor providing services involving PHI is called a Business Associate;
- A covered entity and business associate must enter into a Business Associate Agreement (BAA);
- Business Associates are directly liable for HIPAA compliance and must ensure that their employees or subcontractors receive HIPAA training and employ appropriate safeguards for PHI;
- HIPAA protections apply to a deceased person's PHI for 50 years after they have died.

# HIPAA Security Rule



# HIPAA Security Rule

The HIPAA Security Rule concentrates on safeguarding PHI by focusing on the confidentiality, integrity, and availability of PHI.

- **Confidentiality** means that data or information is not made available or disclosed to unauthorized persons or processes.
- **Integrity** means that data or information has not been altered or destroyed in an unauthorized manner.
- **Availability** means that data or information is accessible and useable upon demand only by an authorized person.



# Security Standards/Safeguards




- APWU Health Plan is required to have administrative, technical, and physical safeguards to protect the privacy of PHI.
- Safeguards must:




  - Protect PHI from accidental or intentional unauthorized use/disclosure in computer systems *(including social networking sites such as Facebook, Twitter and others)* and work areas;
  - Limit accidental disclosures; and
  - Include practices such as encryption, document shredding, locking doors and file storage areas, and use of passwords and codes for access.

# Malicious Software

- Viruses, worms, spyware and spam are all examples of malicious software, sometimes known as "**malware**".
- Safe Internet browsing habits can also reduce the likelihood of an infection; do not open email or click on embedded links from an unknown or untrusted site.
- If the computer or mobile device you are using stores member sensitive information, make sure that your security and anti-virus software is up to date.



# Viruses

- Viruses “infect” your computer by modifying how it operates and, in many cases, destroying data.
- Viruses spread to other machines by the actions of users, such as opening infected email attachments.
- Viruses can forward PHI to unauthorized persons by attaching themselves to documents, which are then emailed by the virus.



- Newer viruses have their own email engines, enabling them to send email without having to use an email client or server.
- Many viruses also install a “backdoor” on affected computer systems allowing for unauthorized access and collection of sensitive information.

# Worms

- Worms are computer programs that can:
  - run independently without user action;
  - spread complete working versions of themselves onto other computers on a network within seconds; and
  - quickly overwhelm computer resources with the potential for data destruction as well as unauthorized disclosure of sensitive information.



# Spyware

- Spyware is software that is secretly loaded onto your computer, monitors your activities, and shares that information without your knowledge.
  - Malicious websites can install spyware on every computer that visits those sites.



**Malicious websites can install spyware on every computer that visits those sites.**

# Spam and Phishing

- **Spam** is an unsolicited or “junk” electronic mail message, regardless of content.
- **Spam** usually takes the form of bulk advertising and may contain viruses, spyware, inappropriate material, or “scams.”



- **Spam** also clogs email systems.
- **Phishing** is a particularly dangerous form of spam that seeks to trick users into revealing sensitive information, such as passwords.

# Safe Browsing Habits

- Safeguard Sensitive Information
  - Look for signs of security when providing sensitive information (i.e.; the web address starts with “https” or a padlock icon is displayed in the status bar).




- Use Security Software
  - The Health Plan uses a variety of antivirus and spyware software that is monitored and kept up to date. Do you?
- Safe Downloading and Streaming
  - When in doubt, just don’t do it!  If a download looks too good to be true, it might be malware.
  - Downloaded files like software or other media can contain hidden malware.
  - Streaming media websites might seem harmless, but watching or listening to streaming media may require downloading a special media player that may contain malware.

# Mobile Devices

- It is strongly recommended that you utilize the following security controls when storing and transmitting sensitive information:
  - Strong power-on passwords;
  - Automatic log-off;
  - Display screen lock at regular intervals while the device is inactive; and
  - Encryption.



**Never** leave mobile computing devices unattended in unsecured areas.

**Remember**, for any mobile device, **encryption** is the best defense!

# Password Control

- **Use strong passwords** where possible, (at least 8 characters, containing a combination of letters, numbers, and special characters).




- **Change your passwords frequently** (every 45-90 days, to prevent hackers from using automated tools to guess your password)



**Many security breaches occur because of bad password habits.**

# Portable Storage Devices

- Whenever possible, avoid using external storage devices to store sensitive information. If you must use such devices, including “thumb” or “flash” drives, use **encryption**, and adhere to the following:
  - Use portable storage media only for transporting information, and not to permanently store information.
  - Once you’ve used the information, erase it from the storage device.
  - Consider attaching your memory stick to your key ring, as you are less likely to lose your keys.



# Communications in Public Areas

- Be aware of your surroundings when discussing Sensitive Information, including PHI. **DO NOT discuss Sensitive Information or PHI in public areas.**



# Best Practice Reminders

- **DO** keep computer sign-on codes and passwords secret, and **DO NOT** allow unauthorized persons access to your computer. Also, use locked screensavers for added privacy.
- **DO** keep notes, files, memory sticks, and computers in a secure place, and be careful **NOT** to leave them in open areas.
- **DO** use encryption when sending or storing PHI on mobile devices, including “thumb” or “flash” drives.
- **DO** hold discussions of PHI in private areas. Also, be aware of places where others might overhear conversations.

# Best Practice Reminders

- **DO** make certain when mailing documents that no sensitive information is shown on postcards or through envelope windows, and that envelopes are closed securely.
- **DO** follow procedures for the proper disposal of sensitive information, such as shredding documents.
- When sending an email, **DO NOT** include PHI or other sensitive information such as Social Security numbers unless you use encryption.



# THANK YOU!

You will receive an email following our Seminar with a link to fill out your class evaluations online.

Please note any questions for the Roundtable discussion on the card provided and place in the drop box at the Registration Desk.

The Roundtable discussion will be during Closing Session:

**Monday, October 28, 2019**

