HIPAA 101

Privacy and Security Training

By: Lisa Banford,
HIM Director,
HIPAA Privacy Officer

Privacy and Security Training

Privacy and Security for all YVFWC Workforce

- Providers
- Staff
- Trainees
- Volunteers
- Contractors/Vendors

Objectives

Privacy and Security Training explains:

- The requirements of the federal HIPAA/HITECH regulations, state privacy laws, and YFVWC policies and procedures that protect the privacy and security of confidential data
- How these affect you and your job
- What information must be protected
- How you can protect confidential and sensitive information
- Your responsibilities for good computer practices
- How to report privacy breaches and security incidents

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that specifies administrative simplification provisions that:

- Protect the privacy of patient information
- Provide for electronic and physical security of patient health information
- Require “minimum necessary” use and disclosure
- Specify patient rights to approve the access and use of their medical information

Privacy is bigger than HIPAA

In addition to HIPAA, there are other federal laws which govern the release of information, mandate that information be protected, and in some cases require that individuals be granted certain rights relative to control and access of their information

- The Medicare Conditions of Participation require that Health Care Facilities promote each patient's rights, including privacy (42 CFR Section 482.13).
- The Federal Trade Commission (FTC) charged with protecting consumers requires banking and other industries to implement "red flag" standards (12 CFR part 681) to detect and prevent identity theft related to customer service accounts. These red flag rules extend to Health Care Institutions
- Federal Department of Health and Human Services (HHS) as well as multiple federal agencies require the protection of the privacy and confidentiality of participants in research clinic trials

YVFWC Policies & Procedures

- YVFWC has policies and procedures to protect privacy and security information
- As a YVFWC employee, you are responsible to follow these policies and procedures to protect the privacy and security of the patient’s medical information

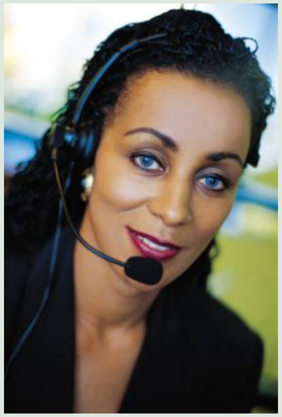
Fines and Penalties

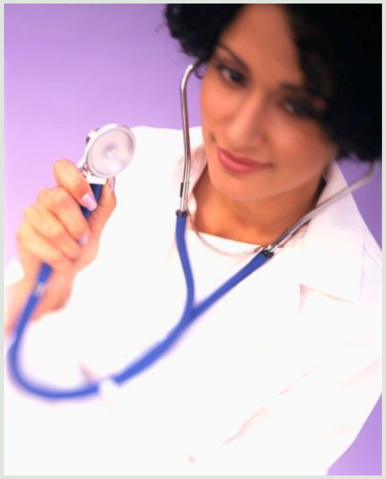
Privacy violations may carry penalties under the federal HIPAA/HITECH, state privacy laws and YVFWC policies:

- HIPAA Criminal Penalties
  - $50,000 - $1,500,000 fines
  - Imprisonment up to 10 years
- HIPAA Civil Penalties
  - $100 - $25,000 fines
  - More fines if multiple year violations
- State Laws
  - Fines and penalties apply to individuals as well as health care providers, up to a maximum of $250,000; may impact your professional license
  - Imprisonment up to 10 years
- YVFWC corrective and disciplinary actions
  - Up to and including loss of privileges and termination of employment

How do the Laws Affect You and Your Job?

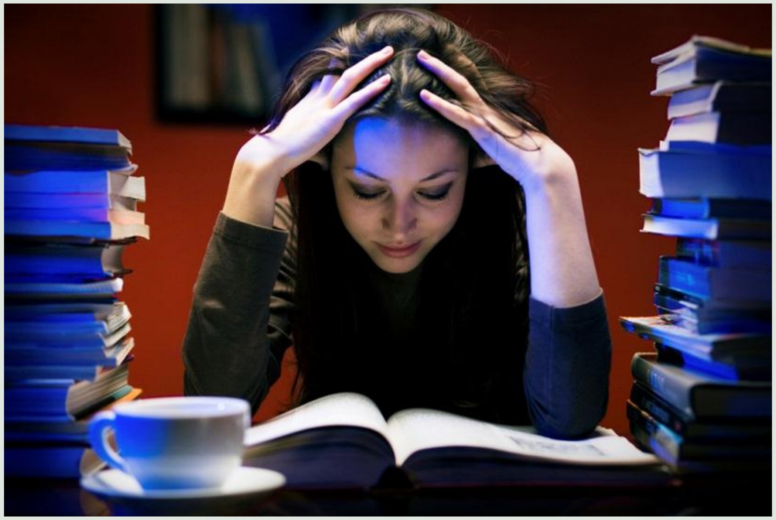
- How do the privacy laws apply to you?
- Who uses PHI at YVFWC?





How the HIPAA Laws Apply to You!

HIPAA requires that YVFWC train all workforce members about the organizations HIPAA policies and procedures which may affect the work you do. These rules apply to you when you look at, use, or share Protected Health Information (PHI).



Who Uses PHI at YVFWC?

- Anyone who works with or may view health, financial, or confidential information with HIPAA protected health identifiers
- Everyone who uses a computer or electronic device which stores and/or transmits information
- The following workforce members:
  - Providers
  - Reception
  - Nursing Staff
  - Volunteers
  - Students
  - Researchers and Staff investigators
  - Accounting, Payroll, and Billing
  - Almost Everyone, at one time or another

Protected Health Information (PHI)

This section explains:

- What information must be protected
- PHI identifiers
- YFWC’s disclosure of PHI policy
- The Notice of Privacy Practices for PHI
- Purposes other than Treatment, Payment, or Operations (TPO)
- Examples of TPO
- Exceptions to the “Minimum Necessary” standard
- When you should view, use, or share PHI

What Information Must Be Protected?

You must protect an individual's PHI which is collected or created as a consequence of a health care provision

- PHI:
  - Is information related to a patient's past, present, or future physical and/or mental health or condition
  - Can be in any form: written, spoken, or electronic (including video, photographs, and x-rays)
  - Includes at least one of the 18 personal identifiers in association with health information
- These rules apply to you when you view, use, and share PHI

Protected Health Information (PHI) Identifiers

- Name
- Postal Address
- All elements of dates except year
- Telephone number
- Fax number
- Email address
- URL address
- IP address
- Social security number
- Account numbers
- License numbers
- Medical record number
- Health Plan Beneficiary #
- Device identifiers and their serial numbers
- Vehicle identifiers and serial numbers
- Biometric Identifiers (finger and voice prints)
- Full face photos and other comparable images
- Any other unique identifying number, code, or characteristic

YVFWC’s Notice of Privacy Practices

- In order for YVFWC to use or disclose PHI:

- YVFWC must give each patient a **Notice of Privacy Practices** that describes how YVFWC may use and disclose the patient’s PHI

- Advises the patient of his/her privacy rights

- YVFWC must attempt to obtain the patient’s signature acknowledging receipt of the Notice, except in emergency situations. If a signature is not obtained, YVFWC must document the reason why it was not.

Notice of Privacy Practices for PHI

The Notice of Privacy Practices (NOPP) allows PHI to be used and disclosed for purposes of TPO

- Treatment (**T**), Payment (**P**), Operations (**O**)
- TPO includes teaching, medical staff/peer review, legal, auditing, customer service, business management, and releases mandated by law
- YVFWC must have a Business Associate Agreement (BAA) with vendors who will use PHI when providing a service to YVFWC

For Purposes Other Than TPO

Unless required or permitted by law, YVFWC must obtain written authorization from the patient to use, disclose, or access patient information.

- **Patient Authorization** allows YVFWC to disclose information for purposes not related to treatment, payment, or operations

Examples of TPO

- The patient’s referring physician calls and asks for a copy of the patient’s recent exam at YVFWC (**Treatment**)
- A patient’s insurance company calls and requests a copy of the patient’s medical record for a specific service date (**Payment**)
- The Quality Improvement office calls and asks for a copy of a patient’s chart for review (**Health Care Operations**)
- For these TPO purposes, patient information may be provided

Except for Treatment, the Minimum Necessary Standard Applies

- For patient care and treatment, HIPAA does not impose restrictions on use and disclosure of PHI by health care providers Exceptions: psychotherapy information, HIV test results, and substance abuse information
- For anything else, HIPAA requires users to access the minimum amount of information necessary to perform their duties. Example: a billing clerk may need to know what laboratory test was done, but not the result

When Should you?

- **View PHI**
- **Use PHI**
- **Share PHI**

Remember

- Use information **only when necessary** to perform your job duties
- Use only the **minimum necessary** to perform your job duties
- Follow YVFWC policies and procedures for information confidentiality and security
- Ask your supervisor for your department's privacy and security procedures

Protecting Privacy

This Section Explains:

- Verbal exchanges
- Knowing where you left your paperwork
- Disposal of paper documents
- Security of Electronic Patient Information (ePHI)
- Privacy breach from lost, stolen, or misdirected information
- Incidents from any format of information

Verbal Exchanges

- Patients may see normal clinical operations as violating their privacy
- Be aware of your surroundings when talking
- Do not leave PHI on answering machines
- Ask yourself, **“What if it was my information being discussed like this?”**

Know Where You Left Your Paperwork

- Check printers, faxes, copier machines when you are done using them
- Ensure paper charts are returned to applicable areas in nursing stations, medical records, or designated areas
- Do not leave hard copies of PHI laying on your desk; lock it up in your desk at the end of the day
- Seal envelopes well when mailing

Disposal of Paper Documents

- Always throw documents with patient information in a shred bin for proper destruction
- Dispose of paper and other records with PHI in secured shredding bins. Recycling and Trash bins are NOT secure.
- Shredding bins work best when papers are put inside the bins. When papers are left outside the bin, they are not secured from: Daily gossip, trash, and the public

Security of Electronic Patient Information (ePHI)

Good security standards follow the "90/10" Rule:

- 10% of security safeguards are technical
- 90% of security safeguards rely on the computer user (**YOU**) to adhere to good computer practices

Privacy Breach from Lost, Stolen, or Misdirected Information

A privacy breach can occur when information is:

- Physically lost or stolen Paper copies, films, tapes, electronic devices
- Misdirected to others outside of YVFWC
- Verbal messages sent to or left on the wrong voicemail or sent to or left for the wrong person
- Mislabeled mail, misdirected email
- Wrong fax number, wrong phone number
- Placed on YVFWC intranet, internet, websites, Facebook, Twitter
- Not using YVFWC secured email tool

Examples of Privacy Breaches

- Talking in public areas, talking too loudly, talking to the wrong person
- Lost/stolen or improperly disposed of paper
- Lost/stolen laptops, PDAs, cell phones, media devices (video and audio recordings)
- Email or faxes sent to the wrong address, wrong person, or wrong number
- User not logging off of computer systems, allowing others to access their computer or system

Your Responsibilities for Good Computing Practice

This section explains:

- Computer security
- Protecting portable devices
- Safe emailing
- Additional security precautions

Computer Security

- Ensure your computer and data are physically secured
- Create a strong password and **do not share** your username or password with **anyone**
- Log off your computer terminal when you are done, or even if you walk away for a few moments
- Ensure information on computer screens is not visible to patients who pass by
- Lock your PC by using the keyboard command Ctrl + Alt + Delete

Additional Security Precautions

- Practice Safe Emailing
- Do not open, forward, or reply to suspicious emails
- Do not open suspicious email attachments or click on unknown website addresses
- NEVER provide your username and password to an email request
- Use secure email when sending anything related to PHI
- It is your responsibility when communicating to send all PHI securely

Reporting Privacy Breaches and Security Incidents

This section explains:

- How to report privacy breaches
- How to report security breaches
- The importance of immediately alerting known or suspected incidents
- Where resources for privacy and security can be found

How to Report Privacy Breaches

- Immediately report any known or suspected privacy breaches (such as paper, conversations, suspected unauthorized or inappropriate access or use of PHI) to the Privacy Office at (509) 248-5277 or ext. 4927

How to Report Security Incidents

- Report lost or stolen laptops, Blackberries, PDAs, cell phones, and flash drives immediately to the YVFWC Help Desk, ext. 2167, and to your supervisor.
- Immediately report any unusual or suspected information security incidents to your Supervisor as well as unusual computer activity

Remember
To the patient, ALL information is private.

- This includes a patient's: Personal information
- Financial information
- Medical information
- Protected Health Information
- Information in any format: spoken, written, or electronic

Resources for Privacy and Security

- Your Supervisor/Manager
- IS Department
- Privacy Office Contact Number: (509) 248-5277 or ext. 4927
- Privacy Officer: Lisa Banford
- Security Officer: Diane Tschauner