HIPAA 101
Privacy and Security Training

Privacy and Security Training

Privacy and Security for New Heritage Healthcare Workforce
• Physicians
• Employees
• Volunteers
• Contractors
• Students
• Trainees
• Contractors / Vendors

Course Objectives

Privacy and Security Training explains:
• The requirements of the federal HIPAA/HITECH regulations, state privacy laws, and practice 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
Privacy and Security
Laws and SJHS Policies

This section explains the following laws and policies:

- Federal HIPAA
- Federal HITECH Act
- California State Medical Information Laws
- SJHS & Heritage Healthcare policies and procedures
- Fines and penalties

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

HITECH Act Updated HIPAA

As part of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act updated federal HIPAA privacy and security standards.

The updates include:

- Breach notification requirements
- Fine and penalty increases for privacy violations
- Right to request copies of the electronic health care record in electronic format
- Mandates that Business Associates are civilly and criminally liable for privacy and security violations
California Medical Information Privacy Laws

• Applies to individuals as well as institutions
• Unauthorized access includes the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment or other lawful use
• When you suspect or know of a breach you must report it to the Privacy Office immediately

Other Federal Laws

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 of and access of their information.

• The Medicare Conditions of Participation require that hospitals 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 and service accounts. These red flag rules extend to Health Care Institutions.
• The Family Education Rights and Privacy Act (FERPA) governs the protection of education records which include student health records (20 USC 1232g). HIPAA specifically exempts individually identifiable health information in education records. As FERPA records are exempt from HIPAA, all releases from education records must be in accordance with FERPA regulations.
• 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 clinical trials.

Privacy is bigger than HIPAA

California State Laws

Confidentiality of Medical Information Act (CMIA) (Civil Code Section 56 et seq.) requires that:

• Confidentiality of Medical Information be protected and establishes protections against disclosures of Individually Identifiable Medical Information
• Institutions notify California residents of breaches of electronic social security number, access codes to financial accounts, medical, and insurance information
• Healthcare institutions implement safeguards to protect the privacy and confidentiality of Medical Information
Lanterman-Petris-Short (LPS) (Welfare and Institutions Code Section 5328 et seq.) provides special confidentiality protections for medical records containing mental health or development disabilities information.

Title 22, California Code of Regulations, Section 70707(b)(8), requires acute care hospitals to protect patient rights to the confidential treatment of all information related to their care and stay at the hospital.

Privacy is bigger than HIPAA

California State Laws

SJHS and Heritage Healthcare

SJHS and Heritage Healthcare have policies and procedures to protect the privacy and security of information.

As a Heritage Healthcare workforce member, you are responsible to follow these policies and procedures to protect the privacy and security of information.

Ask your Supervisor or Manager for guidance.

Remember that privacy applies to ALL verbal, written, and electronic information.

Fines and Penalties

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

- HIPAA Criminal Penalties
  - $50,000 - $1,500,000 fines
  - Imprisonment up to 10 years
- HIPAA Civil Penalties
  - $100 - $25,000 / year 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
- Heritage Healthcare corrective and disciplinary actions
  - Up to and including loss of privileges and termination of employment
How the Laws Affect You and Your Job

This section explains:

• How the privacy laws apply to you
• Who uses PHI at Heritage Healthcare

How the HIPAA Laws Apply to You

HIPAA requires that Heritage Healthcare train all workforce members about St Joseph Health System HIPAA policies and specific 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 Heritage Healthcare?

• 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:
  - All Heritage Healthcare staff
  - All physician staff
  - All contracted and agency employed staff
  - Volunteers
  - Students who work with patients
  - Researchers and staff investigators
  - Accounting and payroll staff
  - Almost EVERYONE, at one time or another
Protected Health Information (PHI)

This section explains:

• What information must be protected
• PHI identifiers
• Heritage Healthcare’s usage or disclosure of PHI
• The Notice of Privacy Practices (NOPP) 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
  • Any health information with identifiers (on the following page) is Protected Health Information (PHI)

Protected Health Information (PHI) Identifiers

The 18 Identifiers defined by HIPAA are:

- 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 number
- Biometric identifiers
- (finger and voice prints)
- Full face photos and other comparable images
- Any other unique identifying number, code, or characteristic
In order for Heritage Healthcare to use or disclose PHI:

- Heritage Healthcare must give each patient a **Notice of Privacy Practices** that:
  - Describes how Heritage Healthcare may use and disclose the patient’s PHI
  - Advises the patient of his/her privacy rights

- The practice must attempt to obtain the patient’s signature acknowledging receipt of the notice, except in emergency situations. If a signature is not obtained, the practice 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
  - Heritage Healthcare must have a Business Associate Agreement (BAA) with vendors who will use PHI when providing a service to Heritage Healthcare.

**Examples of TPO**

- The patient’s new physician calls and asks for a copy of the patient’s recent exam at Heritage Healthcare (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 an diagnostic report (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 Heritage Healthcare policies and procedures for information confidentiality and security
- Ask your supervisor for your department's privacy and security procedures
Scenario 1

I do not work with patients or have access to medical records, however I see patients pass by my desk in the office. Can I talk about the patients with my coworkers, family and friends even if it has nothing to do with my job?

A. You may not discuss any patient information with anyone unless required for your job
B. You may only talk about the patient with our coworkers
C. You may only talk about the patient with your family and friends

Scenario 1 - Answer

The correct answer is A. Information can only be used as needed for your job.

A. You may not discuss any patient information with anyone unless required for your job
B. You may only talk about the patient with our coworkers
C. You may only talk about the patient with your family and friends

Scenario 2

I work in the lab and my friend, who works in another department, told me that she just saw a famous movie star get on the elevator. My friend read in the paper that the movie star has cancer and asked me to find out where she is going. Can I give my friend the information?

A. It is okay as I am only looking up her location, not her medical condition
B. I already have approval to access patient clinical systems, so no one will know that I accessed it
C. It is not necessary for my job, so I would be violating the patient's privacy by checking on her location and by sharing this information with my friend
Scenario 2 - Answer

The correct answer is C.

It is not part of your or your friend's job, even if you are a system user. Your access to the record will automatically be recorded and can be tracked. Both you and your friend are not protecting the privacy of this patient. There could be serious consequences to your employment.

A. It is okay as I am only looking her location, not her medical condition
B. I already have approval to access patient clinical systems, so no one will know that I access it
C. It is not necessary for my job, so I would be violating the patient's privacy by checking on her location and by sharing this information with my friend

Scenario 3

As a file clerk, it is my job to see PHI, but while opening lab reports, I saw my manager's pregnancy test results. Her pregnancy test was positive! I congratulated her, but found out that I was the first person to tell her. Did I do the right thing?

A. It is okay as it was part of my job to see PHI
B. She is an employee at Heritage Healthcare, so it is okay to look at other Heritage Healthcare employee records
C. I should not have used the information as it was not my job to discuss lab results, to provide a diagnosis, or to use her information outside of my job duties

Scenario 3 - Answer

The correct answer is C.

There was impermissible disclosure of her information. Heritage Healthcare employees can also be patients. As such, they have all the same rights to privacy of their information as does any other patient. This was also a violation of Heritage Healthcare policy, which could impact your employment.

A. It is okay as it was part of my job to see PHI
B. She is an employee at Heritage Healthcare, so it is okay to look at other Heritage Healthcare employee records
C. I should not have used the information as it was not my job to discuss lab results, to provide a diagnosis, or to use her information outside of my job duties
Scenario 4

Because I have access to confidential patient information as part of my job, I can look up anybody’s record, even if they are not my patient, as long as I keep the information to myself.

A. True, as long as I do not share this information
B. I can only look at records when it is required by my job
C. I can access hard copy medical charts, but not electronic records, anytime I want

Scenario 4 - Answer

The correct Answer is B.

It is acceptable only when it is necessary for your job and only the minimum information necessary to do your job. Idle curiosity can jeopardize the patient’s privacy and your employment.

A. True, as long as I do not share this information
B. I can only look at records when it is required by my job
C. I can access hard copy medical charts, but not electronic records anytime I want

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 file rooms
- 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**

- Shred or destroy PHI before throwing it away
- 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
  - Daily trash
  - 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
  - Anytime, anywhere - even while on public transportation, crossing the street, in the building, in your office

• Misdirected to others outside of Heritage Healthcare
  - 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 Heritage Healthcare intranet, internet, websites, Facebook, Twitter
  - Not using Heritage Healthcare’s 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, mail, films, notebooks

• Lost/stolen laptops, PDAs, cell phones, media devices (video and audio recordings)

• Lost/stolen zip disks, CDs, flash drives, memory drives

• Hacking of unprotected computer systems

• 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
Scenario 5

I called a patient’s phone number and left a voice mail for Mr. John Smith to contact Heritage Healthcare regarding his scheduled thyroid surgery. Was this a privacy breach?

A. No, the patient provided this phone number
B. Yes, I stated his name and medical procedure
C. No, I did not state the medical reason for the surgery

Scenario 5 - Answer

The correct answer is B. Patient name in conjunction with any medical information constitutes PHI. You do not know who will hear the message; the patient may not have told his family, friend or roommate. It is best practice to leave the minimum amount of information needed: your name, phone number, and that you are from Heritage Healthcare. Never leave PHI on an answering machine. Ask your supervisor for the voice mail procedure in your area.

A. No, the patient provided this phone number
B. Yes, I stated his name and medical procedure
C. No, I did not state the medical reason for the surgery

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 by using lockdown cables, locked drawers, placement in a secured area, etc.
- 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 passersby
  - Use a privacy screen
  - Lock your PC by using the keyboard command Ctrl + Alt + Delete
  - Use a password to start up or wake-up your computer
- Ensure your system has anti-virus and all necessary security patches and updates

Portable Device Security Tips

- Always encrypt portable devices and media with confidential information on them (laptops, flash drives, memory sticks, external drives, CDs, etc.)
- Encryption must be an approved SJHS data encryption solution
  - Check with the IT department. A Heritage Healthcare owned device may have already been encrypted for you.
  - Purchase only electronic devices and media which can be encrypted.

Best Practice: Do not keep confidential data on portable devices unless absolutely necessary. And if necessary, the information must be encrypted.

Additional Security Precautions

- Make sure your computer has anti-virus and all necessary security patches. SJHS IT automatically updates these regularly. Do not interrupt these updates! You can continue to work while they are being installed.
- Do not install unknown or unsolicited programs
- 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
  - Delete spam and empty the “Deleted Items” folder
  - Use a secure email solution whenever sending email outside Heritage Healthcare use [Secure] in the subject line
- It is your responsibility when communicating to send all PHI securely
Scenario 6

A physician is very busy and asks you to log into Touchworks using his user ID and password to retrieve some patient reports. What should you do?

A. It is a physician, so it is okay to do this
B. Ignore the request and hope he forgets
C. Decline the request and refer him to the Heritage Healthcare Information Security Policies
D. None of the above

Scenario 6 - Answer

The correct answer is C. Always login under your own user ID and password. If you do not have system owner permission to access the system, then do not access the system. This would have been a violation of privacy and security policies.

A. It is a physician, so it is okay to do this
B. Ignore the request and hope she/he forgets
C. Decline the request and refer them to the Heritage Healthcare Information Security Policies
D. None of the above

Scenario 7

As part of your job, you need to use a laptop as you work at various Heritage Healthcare sites. You have patient emails, addresses, and medical information files on the laptop. What is the best way to protect this device?

A. The information on my portable device is encrypted, I use a complex password, and I physically secure the device when leaving it unattended
B. I only need a complex password to secure the laptop
C. It is secured as I use a complex password and when unattended, I always lock it up in the trunk of my car
D. None of the above
Scenario 7 - Answer

The correct answer is A.

Your laptop must be encrypted if it contains Heritage Healthcare patient information or other sensitive confidential information. Password protection by itself is not enough but you do need to use complex passwords for the device and physically secure it when unattended. Unencrypted devices are considered unsecured in the event of a loss or theft by federal and state privacy laws and therefore reportable to federal and state agencies!

A. The information on my portable device is encrypted, I use a complex password, and I physically secure the device when leaving it unattended
B. I use a complex password and physically secure the device when unattended
C. It is secured as I use a complex password and when unattended, I always lock it up in the trunk of my car
D. None of the above

Question 1

Which workstation security safeguards are you responsible for using and/or protecting?

A. Your User ID
B. Your Password
C. Logging out of programs that access PHI when not in use
D. All of the above

The correct answer is D.

Always log off programs and always protect your user ID and password. Never share these with anyone.

A. Your User ID
B. Your Password
C. Loggin out of programs that access PHI when not in use
D. All of the above
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 Hotline at 866-913-0275

How to Report Security Incidents

• Report lost or stolen laptops, Blackberries, PDAs, cell phones, and flash drives immediately to YOUR SUPERVISOR or the I/T Helpdesk
  • Immediately report any unusual or suspected information security incidents to your Supervisor including but not limited to the loss and/or theft of any form of PHI (paper, films, etc.) as well as unusual computer activity
  • If no one is available to receive your report, contact the I/T HelpDesk at 877-552-7547
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

---

Question 2

You can protect patient information by:

A. Protecting verbal, written, and electronic information
B. Utilizing safe computing skills
C. Reporting suspected privacy and security incidents
D. Following SJHS and Heritage policies
E. All of the above

---

Question 2 - Answer

The correct answer is **E**. All of these actions helps to protect the privacy and security of patient information.

A. Protecting verbal, written, and electronic information
B. Utilizing safe computing skills
C. Reporting suspected privacy and security incidents
D. Following University policies
E. All of the above
Summary

Remember, HIPAA is not optional. Each one of us has an obligation to protect patient information. Keeping in mind that privacy rights do not prevent us from carrying out every required part of our jobs we need to make sure we never use more than the minimum information in carrying out our work.

Please make certain you have signed in for this session or you complete the signature attestation for completion of this course.

Please Complete the Certification

Please obtain a Course Completion Certificate from your privacy officer, Carol Park or Vicki McKemy to receive credit for this course.

Questions? Tom.Loughrey@stjoe.org

Tom Loughrey
Director of Compliance – Physician Practices
St Joseph Health System