2022
HIPAA Privacy & Security

Adam Kammer
Director, Corporate Compliance and Privacy
Adam.Kammer@stelizabeth.com

Initiation: 2005; Reviewed: 10/2021

Purpose/Objectives

Purpose

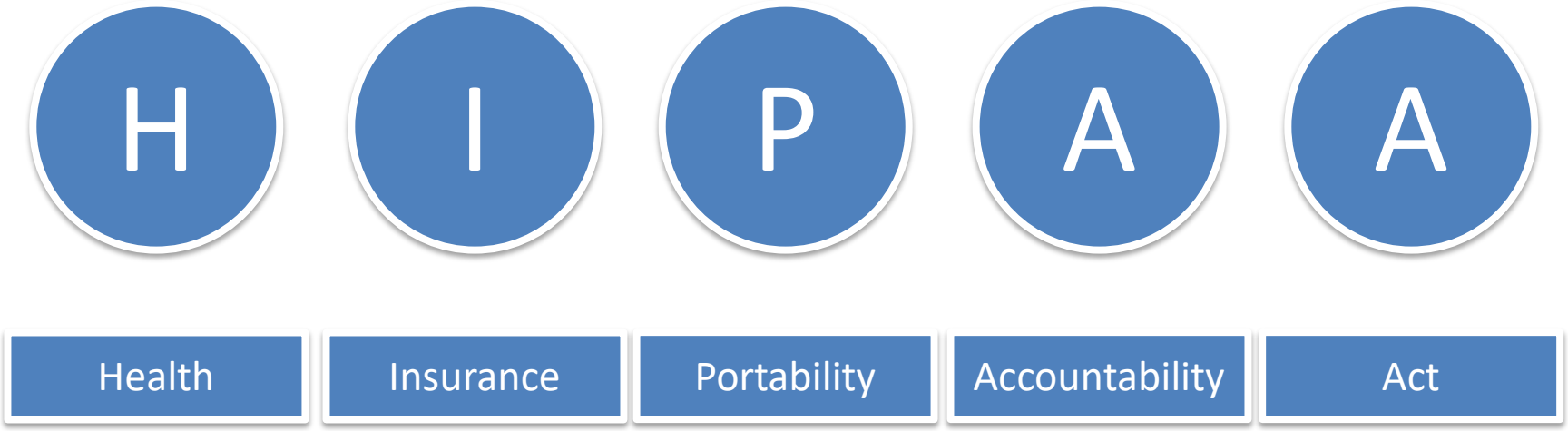
To understand the importance of protecting patient and corporate information.

Objectives

After completing this learning module, the participant will be able to:

- Discuss St. Elizabeth Healthcare's policies.
- Describe how all associates and providers are required to protect patient and corporate information.

Purpose of HIPAA



- Its purpose is to establish nationwide protection of patient confidentiality, security of electronic systems, standards and requirements for electronic transmission of health information.
- Two parts of HIPAA are: (1) Privacy; and (2) Security.
- Healthcare providers are required to train their associates on these regulations.

HIPAA Security and Privacy Officers

Alex Rodriguez
Chief Information Officer/IT Security
Chancellor Data Center
(859) 301-6198

Lisa Frey
Senior Vice President Legal Services/General Counsel
Edgewood Campus
(859) 301-5580

What is Protected Health Information (PHI)?

Protected Health Information (PHI) is any health information that may reasonably identify a patient, such as:

- Name
- Address
- Date of birth
- Telephone Number
- Fax Number
- E-mail address
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Genetic Information
- Finger or voice prints
- Facial Photographs
- Any other unique identifying number, characteristic, or code
- Age greater than 89
- Diagnosis
- Account Number

Protected Health Information continued

We must protect our patients' PHI in **all** forms; including, but not limited to:

- **Verbal** discussions (e.g., in person, on the phone).
- **Written** on paper (e.g., medical chart, progress note, prescription, x-ray order, referral form, invoices, explanations of benefits, scratch paper).
- In all of our **computer applications/systems** (e.g., Epic, Lab, X-ray).
- In all of our **computer hardware/equipment**
- (e.g., PCs, laptops, PDAs, fax machines/servers, thumb drives, cell phones).

The HIPAA Privacy Rule covers (among other things):

I. Patient's Rights

1. Notice of Privacy Practices
2. Obtain access to their PHI
3. Request Additional privacy protection and confidential communication
4. Request an amendment to their PHI
5. Receive an accounting of the uses and disclosures of their PHI
6. Filing a complaint / Breach notification

II. Uses and Disclosures of PHI

III. Minimum Necessary

IV. Reasonable Safeguards

V. Policies, Procedures and Documentation

I. Patient Rights

HIPAA requires St. Elizabeth Healthcare to provide our patients access to our Notice of Privacy Practices.

This Notice:

- Tells patients what St. Elizabeth Healthcare is doing to protect their PHI.
- Tells patients we will use their PHI for payment, treatment, and healthcare operations.
- Informs patients about their privacy rights.
- Explains to patients how they can exercise their privacy rights.
- Provides the title and phone number of a contact person if the patient wants more information or wishes to file a complaint.

Patient Rights:
1. Notice of Privacy Practices

The "Notice of Privacy Practices" is presented to each patient as they are registered. The notice informs the patient of the following rights (among others):

- Receive the Notice of Privacy Practices.
- Obtain Access to their PHI.
- Request Additional Privacy Protections and Confidential Communications.
- Request an Amendment to their PHI.
- Receive an Accounting of the Uses and Disclosures of their PHI.
- Be notified if there is a Breach of their Unsecured PHI.

Patient Rights:
2. Obtain Access to PHI

As a general rule, Patients have the right to inspect and copy their PHI

Situations where access may be denied or delayed:

- Psychotherapy notes.
- When PHI was compiled for civil, criminal or administrative action or proceedings.
- When access would be prohibited by law.
- When access reasonably could/would endanger another person's life, health or safety.
- When a research study denies the individual access.
- When PHI was obtained under a promise of confidentiality and access would reveal the source of the PHI.

Patient Rights:
3. Alternative Communications

Patients have the right to request to receive communication by alternative means or location.

Examples:

- The patient may request a bill be sent directly to him or her instead of to an insurance company.
- The patient may request we contact him or her on a cell phone instead of at a home telephone number.

Patient Rights:
4. Amendment Requests

Patients have the right to request an amendment or to correct their medical record.

- Situations where a request may be denied.
  - St. Elizabeth Healthcare did not create the information.
  - The record is accurate and complete according to the health care professional who wrote it.

- A patient states there is an error in his or her medical record and wants it corrected. What should you do?
  - Give the patient the contact information for the HIPAA Privacy Officer to request to have the record amended.

Patient Rights:
5. Accounting of Disclosures

- Patients have a right to ask for an accounting of disclosures of their medical information (for as far back as six years). This report lists the places where the St. Elizabeth has disclosed PHI for purposes other than payment, treatment or health care operations.
- As a St. Elizabeth Healthcare associate, you may be required to account for disclosures. Examples of potential areas where accounting of disclosures applies are: Public Health Authorities, Health Oversight, Judicial Proceedings, Law Enforcement. Ask your supervisor if your job requires you to account for disclosures.

Patient Rights:
6. Complaints / Breach

- Patients have the right to file a privacy complaint.

  Direct all requests or complaints regarding HIPAA Privacy Rights to the Privacy Officer at (859) 301-5580.

- Patients have the right to be notified if there has been a breach of their unsecured PHI.

II. Uses and Disclosures of PHI

Use: when we review or use PHI internally (treatment, audits, training, customer service, quality improvement).

Disclosure: when we release or provide PHI to someone (e.g., an attorney, a patient, faxing records to another provider, etc.).

Note: St. Elizabeth is permitted to use and disclose PHI, without obtaining authorization from the patient, for payment, treatment, and healthcare operations.

Uses and Disclosures of PHI (continued)

A patient signs an "Authorization to Use or Disclose PHI" form which allows St. Elizabeth Healthcare to use and disclose PHI for purposes other than payment, treatment or healthcare operations.

- Authorizations are obtained on a case-by-case basis and are needed each time a different use or disclosure is desired.
- Before any PHI is released, associates must follow facility procedures for verifying the identity of the person requesting the information.
- After an Authorization is provided, the patient can later revoke or cancel the Authorization.

III. Minimum Necessary

The minimum necessary standard requires St. Elizabeth Healthcare associates to access or disclose the least amount of PHI possible to accomplish their jobs.

The minimum necessary standard does not apply when information is requested to treat a patient.

IV. Reasonable Safeguards

HIPAA requires us to use **"reasonable safeguards"** to protect our patients' PHI. "Reasonable Safeguards" include:

- Do not discuss a patient with another associate unless you are both involved in that patient's care.
- When you do discuss patients, do so in a private place, when possible. If you need to speak in a public area, keep your voice down.
- Do not view the medical records of anyone who is not your assigned patient.
- Do not leave computer screens unattended or aimed in a direction where patients or visitors can view them.

Reasonable Safeguards, continued

- To the extent possible, avoid the use of PHI on boards in areas viewable by the public. Where such boards must be used, limit information to the minimum necessary.
- Avoiding leaving papers containing PHI on desks or other surfaces in plain view of others.
- Keep records and papers in file cabinets or drawers when not in immediate use.
- Place paper/printed materials in the shredding containers when they are no longer needed (never place them in the trash can).
- Pull the curtain and speak quietly when discussing a patient's condition or treatment in a semi-private room or when visitors are present.

V. Privacy Policies, Procedures and Documentation

- As part of the HIPAA Privacy Rule, St. Elizabeth Healthcare is required to have written policies and procedures relating to PHI and information practices.
- The HIPAA Privacy policies and procedures can be located in Compliance 360, in the HIPAA Privacy folder.

Associate Access of PHI

- **ASSOCIATES MAY NOT** use the St. Elizabeth Healthcare computer system to access medical records or financial records of themselves, their children, their spouse, their neighbors, their co-workers or anyone else, without a business based reason to do so. Nor may they view the paper records of any of these individuals without a business-based reason to do so.

- Policy HIPAA-A-08 states: "associates … may not use the privileges associated with their position to view their own PHI, nor the PHI of family or friends."

- **St. Elizabeth Healthcare takes violations of this policy very seriously**. We audit computer usage, so we know when associates have accessed information and what information was accessed. When it is determined that an associate has accessed PHI without a business-based reason to do so, **discipline will be issued.**

Associate Access of PHI (continued)

- ASSOCIATES MAY NOT access their own PHI or someone else's (co-worker, children, spouse, friend or anyone else) without a business based reason to do so. If it is not your job, you can't do it.
- ASSOCIATES MAY NOT access their own PHI or anyone else's at any time for any non business-based reason including at the inappropriate request of someone else (such as a co-worker or family member, or a physician asking an associate to access or copy his or her own records).
- ASSOCIATES MAY NOT use the privileges associated with their position to view their own PHI nor the PHI of family, friends or co-workers, even in training (i.e., associates may not use their own account or the account of a co-worker to perform Epic training).
- **If there is any doubt in your mind about whether you may access PHI, ask your supervisor or the HIPAA Privacy officer.**

Associate Access of PHI (continued)

There are approved ways for associates to review the PHI of their children and spouse (with the spouse's authorization).

- The patient (or custodial parent in the case of a minor) completes an "Authorization to Obtain/Use or Disclose Protected Health Information (PHI)," which is available in Health Information Management (HIM or "Medical Records") and online at www.stelizabeth.com.

- The patient signs the authorization notifying our HIM department to disclose the information. The associate does not access this information via a St. Elizabeth Healthcare computer -- HIM provides a copy of the appropriate information to the patient (or spouse if so authorized).

Breach Notification

- A privacy breach is an unauthorized disclosure of personal confidential information that violates state or federal privacy laws. St. Elizabeth Healthcare investigates all alleged breaches of personal confidential information reported by its employees, staff of its business associates, or other persons and will work to resolve the issues raised in order to safeguard individuals' confidential information and improve St. Elizabeth business systems and practices.

- The Privacy Officer determines the appropriate level of response (including, as necessary, notification of patients) to mitigate potential harm when St. Elizabeth is made aware of a privacy breach.

Breach Notification continued

St. Elizabeth associates must provide immediate notice to the HIPAA Privacy Officer of any suspected or actual breach of security or unauthorized disclosure of information.

- This includes misdirected faxes and printed PHI inadvertently given to the wrong patient. Staff should make reasonable efforts to **retrieve the information** from the person who inappropriately received it (versus telling the person to shred or destroy it).

Business Associates

A **Business Associate** is "a person or organization that uses or receives PHI from a facility in order to perform or assist the facility with some activity or function."

- Some of St. Elizabeth Healthcare's Business Associates include: Independent Contractors, Consultants, Lawyers, Auditors, Information System/Data Processing Vendors and Billing Companies.
- For a facility to disclose PHI to a Business Associate, a written contract, agreement or other arrangement must be in place that meets regulatory standards and requirements.

Asking Questions & Reporting Concerns

- Associates should report promptly and in good faith any potential violations of the HIPAA Privacy Rule.

- A three-step reporting process was developed to help resolve issues, answer questions or provide a means to report concerns:

    1. Contact your supervisor. If your supervisor is unable to solve the problem, contact their supervisor.

    2. If you feel your problem has not been resolved, or if you would rather not report the issue to a supervisor, call Lisa Frey, the HIPAA Privacy Officer, at **(859) 301-5580**.

    3. You may want to report a situation without revealing your identity. For those concerns, call the Compliance Line at **1-877-815-2414**.

About the Compliance Line

- The Compliance Line is a toll-free 24-hour hotline. The number is **1-877-815-2414.**
- Operators from an outside company make a complete report of your issue and send it to our Corporate Compliance Officer to resolve.
- All calls are confidential. You do not need to give your name if you would prefer not to. Our Compliance Line does not use Caller ID and does not try to trace calls.

No Retaliation Policy

- We forbid retaliation against anyone who reports a concern in good faith.
- Making a good faith report will not put your job at risk. We protect every associate who reports a concern in good faith.
- Anyone who retaliates in any way is subject to immediate discipline (up to and including termination).
- Report retaliation concerns immediately to the Corporate Compliance Officer at **(859) 301-5580**.

Information Security

Electronic information is data created, received, stored or transmitted electronically. SEH has categorized its data systems as follows:

Data Category	Type	Examples
Level I	**Public**	Public Internet Information, Press Releases
Level II	**Internal Use Only**	Normal office documentation with restrictions based on user or group. No appreciable harm could come to the organization if this information was made public.
Level III	**Confidential**	Electronic information that is restricted to a select set of employees. If the information is made public it could negatively impact the organization.
Level IV	**Confidential & Sensitive**	Electronic information that is legally protected or restricted such as Personally Identifiable Information (PII), Protected Health Information (PHI) or Credit Card information. If the information is made public it could negatively impact the organization.

Electronic Media

Electronic media is any device that can store electronic information.

computer networks	computers (PC's, Laptops, Tablets)	smart phones	magnetic tapes	disks	CD's / DVD's	memory drives or devices

NOTE: Department manager approval is required prior to placing PHI onto any portable device or electronic removable media. All such devices must be encrypted before any PHI is placed onto them.

Password Expectations

- Keep your passwords confidential.
- Avoid maintaining a paper record of passwords.
- Change passwords when there is an indication of compromise or when necessary to share with Information Systems for troubleshooting a problem with your computer.
- Do not use the same passwords for business and personal accounts.
- Change passwords at regular intervals (90 days).
- Do not include passwords in any automated log-on process, including web pages.

Passwords (continued)

Password requirements:

- A minimum length of 8 characters.
- Incorporate at least **3** of the **4** following characteristics:
  1. lower case letters (a-z)
  2. upper case letters (A-Z)
  3. numbers (0-9)
  4. punctuation or characters

  (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; " ‘ | \ / ? < > , . ~ `)
- **Do not use** words that are found in a dictionary.
- No personal information such as: names, pets, birth dates, etc. that can be easily guessed.
- **Examples of good passwords:**
  - %mhi30yo% (% my husband is 30 years old %)
  - mVi0521! (my Vacation is 0521 !)

Computer Access

Access to confidential information and **electronic information** are granted to individuals on a need-to-know basis.

If you believe that someone else is inappropriately using your ID or password, immediately notify the Information Systems Service Desk.

The Health System's workforce members will take all reasonable and required precautions to protect the confidentiality, integrity, and accessibility of confidential information.

Computers will not be used to engage in any activity that is illegal under local, state, federal, or international law or in violation of the Health System's policy.

Do not access inappropriate or offensive websites, engage in gambling, send malicious emails, or download copyrighted materials.

Social Engineering

Social engineering is a term used for tricking someone into giving out information like passwords that will compromise system security.

- Note: Don't be afraid to ask questions as to why someone is accessing a PC if they look out of place.
- Notify your supervisor, Security department or Information Systems service desk to report any suspicious activity.
- Here are some **tricks** used by social engineers:
    - An unknown person (with or without a Health System badge) asks for your ID code and password.
    - Someone without an ID badge is using (or attempting) to use a PC without approval.
    - Someone asks for your ID Code and password by phone.

Phishing Attacks

When internet fraudsters impersonate a business to trick you into giving out your personal information, it's called phishing.

Do not reply to email, text, or pop-up messages that ask for your personal or financial information. Do not click on links within them either – even if the message seems to be from an organization you trust. It isn't.

Legitimate businesses do not ask you to send sensitive information through insecure channels.

If you suspect a phishing e-mail, forward the e-mail to mail.admin@stelizabeth.com or contact the IS service desk at 859-301-2541.

Locking the Computer

When leaving a computer unattended, **lock** the computer or **log-off**. (If you share a computer, log off when you are finished, do not lock the computer. If your computer does not have the ability to lock, log out of your system).

To lock the computer:

- Press CTRL, ALT, Delete keys on the keyboard to lock the computer.
- On the pop up window, click on the Lock Computer button.

Destruction of Electronic Media

Destruction of Electronic Media is accomplished in the following ways:

- Place all removable media such as CD's or DVD's into the HIPAA recycling containers.
- Call the IS service desk to arrange a pickup for computer equipment no longer in service.

Reuse of Storage Devices or Removable Media

- It is ok to re-use media within the Health System (take precautions such as reformatting before re-using).
- No storage devices are to be re-used outside of the Health System.
- Any media that cannot be re-used within the Health System should be disposed of.

Confidentiality Extends to the Home

If St. Elizabeth Healthcare allows you to perform your work from home, you are responsible for maintaining the privacy and security of all confidential materials e.g. patient charts, computers and confidential working papers.

All confidential materials should be kept in a location that is not accessible to others.

Using and Transporting Electronic Information Off-Site

- Confidential information (either documents or electronic information) is not to be removed from St. Elizabeth Healthcare without prior approval.
- When approved, electronic information that is to be taken offsite must be stored on approved encrypted media. (Examples are: An "Iron Key" USB device or Laptop that is encrypted.)
- Maintaining the privacy and security of all confidential information that you transport, store or access off-site is your responsibility.

Data Backup

If you have access to the Information Systems network, store electronic information in your network directory folder. Think of this as your “S” or “H” drive. (Information systems backs up the network directories on a nightly basis.)

Do **NOT** store electronic information on local PC’s. It is not secure and it is not backed up. Think of this as your “C” or “D” drive.

Electronic Information Access Auditing:

All St. Elizabeth Healthcare computer systems are subject to a regular audit review.

- The audit review may include:
  - Electronic information that you have accessed.
  - Internet sites that you accessed.

Software/Hardware Protection

Antivirus Software

Anti-virus software is present on all required information systems.

Never bypass or disable anti-virus software.

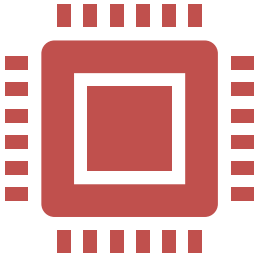
Email Protection

Email attachments are scanned for viruses prior to delivery.

Delete emails before opening when they appear suspicious, or if you don’t know the sender.

If you suspect or detect a problem, notify the IS Service Desk.

Software/Hardware Protection continued



Hardware Protection

Do **not** install hardware of any kind.

Software Protection

Do **not** install personal software or download Internet software.

Downloading Internet software onto your computer may install spy-ware without your knowledge and cause programs to run slower or not function properly.

INCIDENT RESPONSE!

All associates are expected to report any violation of security or privacy policy to Information Systems, the Information Systems Security Officer, Human Resources, or Corporate Compliance.

All incidents, threats, or violations that affect or may affect the information protected by regulatory legislation such as (but not limited to): HIPAA, HITECH, PCI, etc. are reported in the following manner:

1. SEH workforce members notify the Information Service Desk for issues involving viruses, local attacks, denial of service (DOS) attacks, etc. If the helpdesk is not available, workforce members contact the Telephone Services operator and have the Information System's on-call staff notified.

2. The Service Desk or "on-call" staff notifies the CSIRT (Computer Security Incident Response Team).

3. The CSIRT team investigates the incident and coordinates with the ISO (Information Security Officer). Recommendations are communicated through the ISO according to the specific IRP (Incident Response Plan) in use.

INCIDENT RESPONSE! continued

4. The CSIRT team, along with affected departments aggregate and assess the severity of security incidents. These incidents are reported to the ISO. Incidents that should be reported include, but are not limited to:

5. All correspondence with outside authorities (such as local police, FBI, media, etc.) goes through the Corporate Compliance Officer.

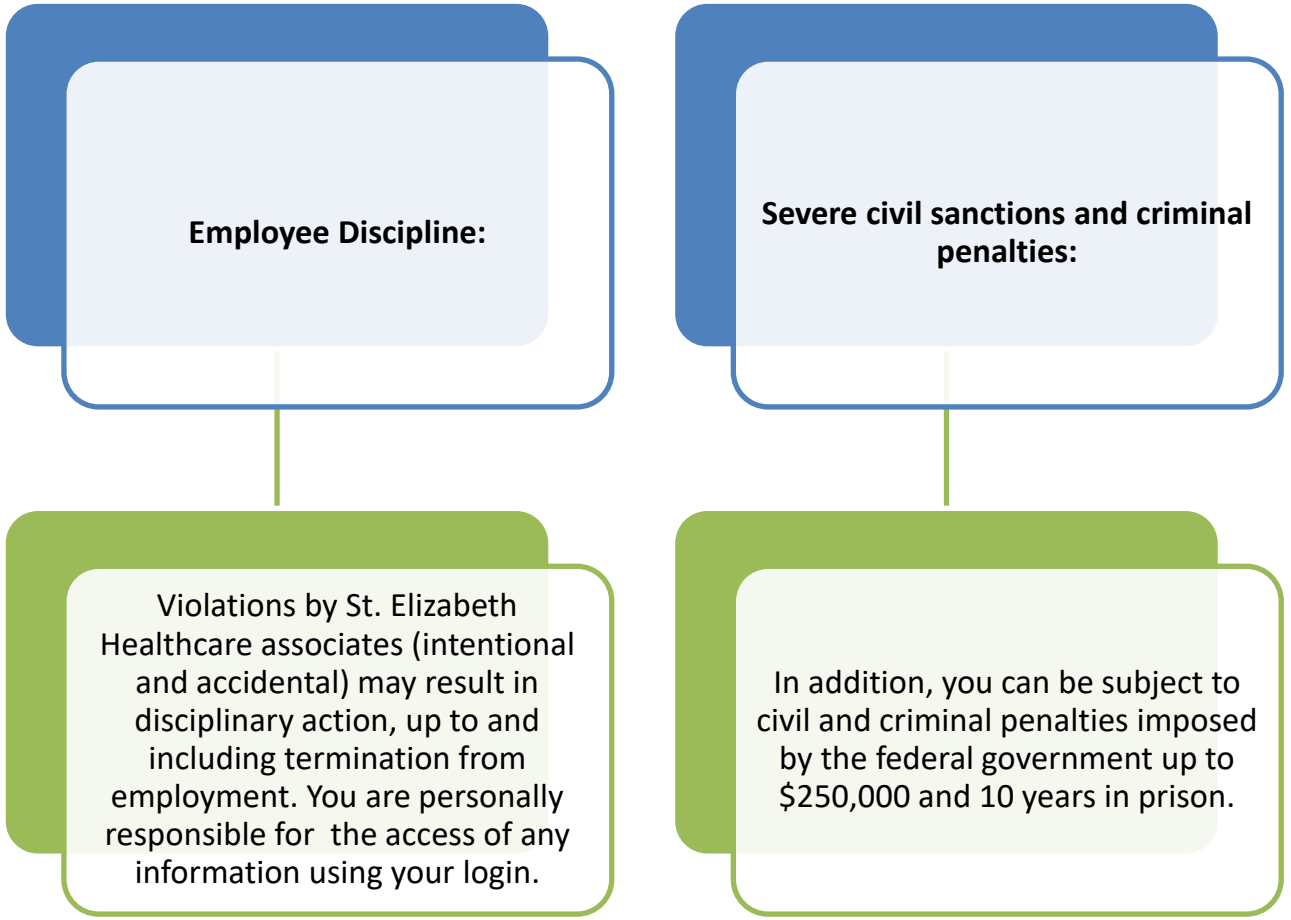
- Virus, worm, or other malicious code attacks
- Network or system intrusions
- Persistent intrusion attempts from a particular entity
- Unauthorized access to information.
- Data loss due to disaster, failure or error

PCI (Payment Card Industry) Security Awareness

Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.

- Any SEH associate that accesses and/or handles payment card data must be approved by their manager and documented within the SEH System Access Request (SAR) repository.
- Any possible security breach related to the confidentiality, integrity or availability of PCI data must be immediately reported to the Information Systems Help Desk (859-301-2541).
- All SEH associates that access and/or handle payment card data are required to change their unique password every 90 days.
- Each SEH associate who accesses and/or handles payment card data is trained on payment card data handling procedures.
- Each SEH associate who accesses and/or handles payment card data completes an annual payment card data computer based training (CBT) module on the proper procedures to handle, transmit or receive payment card data.

Penalties for Non-Compliance



Compliance 360 Policies

- HIPAA-A-01-Authorization Requirements
- HIPAA-A-02-Amendment of Protected Health Information (PHI)
- HIPAA-A-03-Access to PHI
- HIPAA-A-04-Accounting of Disclosures
- HIPAA-A-05-Associate Responsibilities/Agreement
- HIPAA-A-06-Auditing of Compliance
- HIPAA-A-07-Associate Orientation/Training/Documentation
- HIPAA-A-08-Associate Access to PHI
- HIPAA-A-09-Administrative Requirements
- HIPAA-B-01-Breach Notification
- HIPAA-B-02-Business Associates
- HIPAA-C-01-Confidential Communications
- HIPAA-C-02-Confidentiality Agreement with Non-St. Elizabeth Healthcare Associate
- HIPAA-C-03-Confidential Information and Equipment in Public Areas
- HIPAA-D-01-Disclosure of PHI Relating to Medical Center Associates
- HIPAA-D-02-Disclosure of PHI to Personal Representatives
- HIPAA-D-03-Disclosures to Correctional institutions or Other Law Enforcement Custodial Situations
- HIPAA-F-03-Facsimile (FAX) Transmission
- HIPAA-H-01-HIPAA Complaints/Incident Reporting
- HIPAA-H-02-HIPAA Related Record Retention, Storage and Disposal
- HIPAA-I-01-Involvement in Care (Next of Kin) and Notification Purpose
- HIPAA-I-02-Incidental Use and Disclosure of PHI
- HIPAA-M-01-Minimum Necessary/Need to Know
- HIPAA-N-01-Notice of Privacy Practices
- HIPAA-P-04-Policies and Procedures
- HIPAA-R-02-Restriction of Use or Disclosure
- HIPAA-R-03-Refrain From Retaliation
- HIPAA-V-01-Verification of Person (s) Requesting PHI