Information Privacy and Security

2015

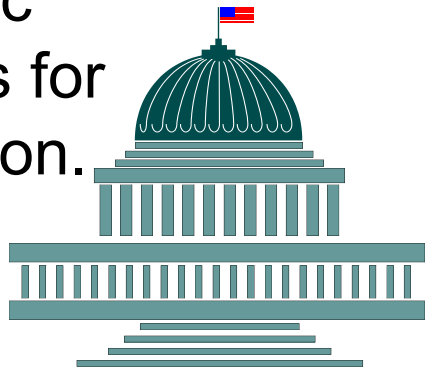
better together

Purpose of HIPAA

"**HIPAA**" stands for the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct.

- Its purpose is to establish nationwide protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.
- The two parts of HIPAA are:

  (1) Privacy and (2) Security
- Healthcare providers are **required** to train their associates and **volunteers** on these regulations.



HIPAA Security and Privacy Officers

Harold Eder, Security Officer
Chancellor Data Center
(859) 301-2916

Lisa Frey, Privacy Officer
Edgewood Campus
(859) 301-5580

What is Protected Health Information (PHI)?

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

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

HIPAA protects PHI in any form, whether verbal, electronic, paper, or computer storage.

Patient Rights – Notice of Privacy Practices

- HIPAA requires St. Elizabeth Healthcare to provide our patients access to our Notice of Privacy Practices (referred to as the "Notice").

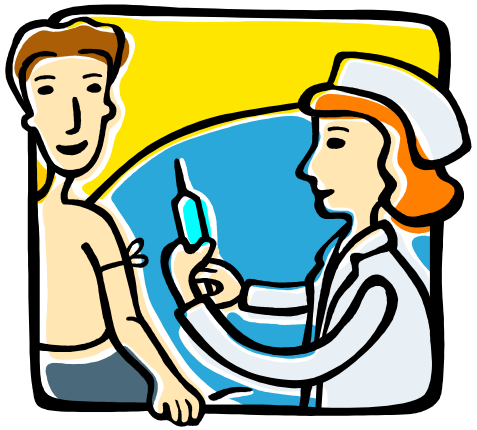
The Notice:

- Tells patients what St. Elizabeth Healthcare is doing to protect their PHI.
- Tells patients we will use their PHI for treatment, payment 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 (continued)

- The “Notice” of privacy practices is presented to each patient as they are registered. The notice informs the patient that they have a right to:

  - Receive the Notice of the Privacy
  - Practices Request Additional Privacy Protections and Confidential Communications.
  - Obtain Access to their PHI.
  - 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

- Patients can request to receive communication by **alternative** means or location.

  For Example:
  - Request are contacted on a cell phone instead of a home number
  - Request that a bill be sent directly to him or her instead of to an insurance company

Accounting of Disclosures

- Patients have a right to ask for an accounting of disclosures of their medical information. This is a report that lists the places where St. Elizabeth has disclosed patient information for purposes other than payment, treatment or health care operations.
- All St. Elizabeth Healthcare associates are required to account for disclosures. Some examples where accounting of disclosures applies are:
    - Public Health Authorities
    - Health Oversight
    - Judicial Proceedings
    - Law Enforcement

Patient Rights: Complaints

- 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.

Uses and Disclosures of PHI

- **USE:** when we review or use PHI internally (such as for treatment, audits, training, customer service, or quality improvement).
- **DISCLOSURE:** a when we release or provide PHI to someone (for example an attorney, a patient, faxing records to another provider,).

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

Uses and Disclosures of PHI

- A patient signs an “Authorization to Use or Disclose PHI” form which allows the Health System 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 revoke** or cancel the Authorization.

Minimum Necessary Standard

- The minimum necessary standard requires St. Elizabeth Healthcare associates to access and give out the **least amount of PHI** possible to accomplish their job.

- The minimum necessary standard does **NOT apply** when information is requested to treat a patient.

Reasonable Safeguards

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

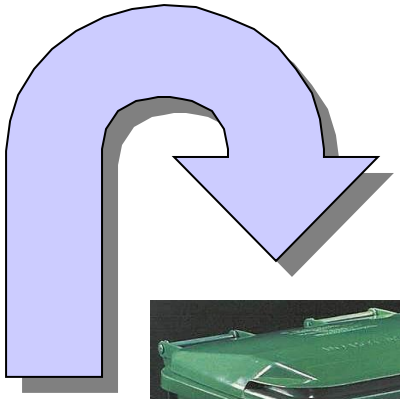
- Do **NOT** discuss a patient with another associate or volunteer unless you are both involved in that patient's care.
- When you do discuss patients, do so in a **private place,** when possible. If you need to speak in a public area, keep your voice down.
- Do **NOT** view the medical records of anyone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

Reasonable Safeguards

Do NOT discuss anything with anyone that you have observed while volunteering that involves a patient outside of St. Elizabeth.

- Sharing with friends a situation with a patient that you saw when volunteering – even if you do not use any names.
- Mentioning to your parents/spouse/friend/priest that you saw someone in the hospital – that is a breach of confidentiality and a HIPAA violation.

Dispose of PHI by putting in a shredding container



NEVER throw PHI in a garbage can

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. All can be found on the St. Elizabeth *intra*net.
- Please **ask** any Volunteer Staff person for assistance in accessing and reviewing these policies and procedures.

Privacy Policies – Access of PHI

- Associates/Volunteers may **NOT** use the St. Elizabeth Healthcare computer system to **access medical 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.
- **St. Elizabeth Healthcare takes violations of this policy very seriously**. If it is determined that an associate/volunteer has accessed PHI without a business-based reason to do so, **discipline will be issued.**

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 reported.

- St. Elizabeth will work to **resolve the issues** raised in order to safeguard individuals' confidential information and improve St. Elizabeth business systems and practices.
- St. Elizabeth's Privacy Officer determines the appropriate level of response (including notification of patients as necessary) to **mitigate potential harm** when St. Elizabeth is made aware of a privacy breach.

Breach Notification

- 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**. It is **NOT** sufficient to simply retrieve the information from the person who inappropriately received it.

Business Associates

- A **Business Associate** is "a person or organization that uses or receives PHI in order to perform or assist the facility with some activity or function."
- A **written contract** must be in place with any Business Associate that meets regulatory standards and requirements for PHI to be released.
- Some of St. Elizabeth Healthcare's **common Business Associates** include:
  - ✓ Independent Contractors,
  - ✓ Consultants,
  - ✓ Lawyers
  - ✓ Auditors,
  - ✓ Data Processing Vendors
  - ✓ Billing Companies

Asking Questions & Reporting Concerns

- Associates should **report promptly and in good faith** any potential violations of the HIPAA Privacy Rule.
- There is a **three-step reporting process** to help resolve issues, answer questions or provide a means to report concerns.

3-Step Reporting Process reviewed in Corporate Compliance module.

Electronic Protected Health Information

Electronic Protected Health Information or **EPHI** is PHI created, received, stored or transmitted electronically.

- Access to confidential information and **EPHI** is granted to associates on a need-to-know basis only.
- Examples of EPHI include, but are not limited to:
  - ✓ Demographic information about a patient contained in information systems such as registration and billing systems.
  - ✓ A note regarding a patient stored in a smart phone.
  - ✓ A digital radiograph of a patient stored on a computer hard drive.

Passwords

Passwords are a very important part of EPHI security

Password Expectations

- Keep your passwords confidential.
- Avoid maintaining a paper record of passwords.
- Change passwords after sharing with Information Systems when they fix a problem with your computer.
- Change passwords at regular intervals (90 days).

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

A Good Password

SEH Password requirements:

- Use at least 3 of the following:
  - ✓ upper (A-Z) and lower case letters (a-z)
  - ✓ numbers (0-9)
  - ✓ punctuation or characters

  (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ `)
- **Do Not** use words found in a dictionary (like WELCOME)
- Not be personal information such as: names, pets, birth dates, etc. because they can be easily guessed.
- **Good Examples :**
  - %msi20yo% (% my spouse is 20 years old %)
  - mVi0521! (my Vacation is 0521 !)

Keep your password Confidential

Computer Use

- Workstations will be used **only for authorized business purposes** related to the duties and responsibilities of Health System associates.
- Do **NOT** access any information unless you need to for your position.
- All associates will take all reasonable and required precautions to protect the confidentiality, integrity, and accessibility of confidential information.
- Do not use computers to access any inappropriate or offensive websites, engage in gambling, send malicious emails or download copyrighted materials.
- When leaving a computer unattended, lock the computer" or log-off.

Social Engineering

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

✓ **Don't be afraid to ask questions as to why someone is using a PC if they look out of place.**

✓ **Notify your supervisor, Security or the Information Systems Help 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.

Using & Transporting PHI Off-Site

Confidential information, ***including hand written notes*** or EPHI, is **not** to be removed from St. Elizabeth Healthcare without prior approval.

EPHI Access Auditing

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

- The audit review may include:
  - ✓ EPHI that **you** have accessed.
  - ✓ Internet sites that **you** accessed.

Virus Protection

- Do **not** install hardware or screensavers of any kind.
- Never bypass or disable anti-virus software – which is present on all St. Elizabeth computer systems.
- Delete suspicious emails BEFORE opening

If you suspect or detect a problem, notify the Information Systems Help Desk

HIPAA Penalties for Non-Compliance

Associate/Volunteer Discipline:
Violations by St. Elizabeth associates may result in disciplinary action, up to and including termination from employment or volunteering with St. Elizabeth Healthcare. You are personally responsible for the access of any information using your login.

Severe civil and criminal penalties:
In addition, you can be subject to civil and criminal penalties imposed by the federal government including fines and prison.

HIPAA Review

1. What is PHI?

   A. **Personal health information**
   B. **Public highway inspector**
   C. **Protected health information**
   D. **Private health institution**

HIPAA Review

2. You are walking down the hall and over-hear health information being discussed between a family and a care provider. The proper reaction would be to:

   A. **Turn them into the Security Officer**
   B. **Approach them and ask who they are talking about**
   C. **Keep the information confidential**
   D. **Call the local papers and turn the health system in for breach of privacy**

HIPAA Review

3. As a volunteer of the Health System, you have access to all health information.
   A. **True**
   B. **False**

HIPAA Review

4. As a volunteer of the Health System, you can NOT look up yourself or anyone in your family on the computer system.

   A. **True**

   B. **False**

HIPAA Review

5. As a St. Elizabeth volunteer you are required to:
   - A. **Maintain privacy for patients as they receive care**
   - B. **Help protect the confidentiality of information that patients give you as a service provider**
   - C. **Not seek out information about patients unless it is related to your volunteer position or job**
   - D. **All of the above**

HIPAA Review

6. The privacy rules only apply to written health information.
   A. **True**
   B. **False**

HIPAA Review

7. Which of the following is not PHI?
   A. **Address**
   B. **Social Security Number**
   C. **Favorite Restaurant**
   D. **Telephone Number**

HIPAA Review

8. Which of the following describes the function of the Notice of Privacy Practices offered to all patients?

   A. **Lets patients know what St. Elizabeth is doing to protect their PHI.**
   B. **Informs patients about their privacy rights**
   C. **Explains to patients how they can exercise their privacy rights**
   D. **All of the above**

HIPAA Review

9. St. Elizabeth must maintain an "accounting of disclosures" when PHI is disclosed for purposes other than payment, treatment and healthcare operations.
   A. True
   B. False

HIPAA Review

10. The minimum necessary standard allow St. Elizabeth volunteers to view all PHI even if it is not related to their job/volunteer function.

    A. **True**
    B. **False**

HIPAA Review

11. EPHI is Protected Heath Information created, received, stored or transmitted electronically.
    A. **True**
    B. **False**

HIPAA Review

12. Which of the following is not an example of electronic media?

A. **Patient education brochures**
B. **Compact disks (CDs)**
C. **Personal computers**
D. **Magnetic tapes**

HIPAA Review

13. Which of the following does not describe St. Elizabeth's password practices?
    A. **Passwords are a minimum of 8 characters.**
    B. **Passwords incorporate multiple characteristics of upper and lower case letters, numbers or punctuation marks.**
    C. **Passwords are words that cannot be found in a dictionary.**
    D. **Passwords are easily guessed so they will not be forgotten.**

HIPAA Review

14. Which of the following best describes St. Elizabeth's Computer Access policy?

    A. **Computers can be used for personal purposes.**
    B. **Associates can access all EPHI even if they don't have a need-to-know purpose**
    C. **There is no need for associates to take reasonable and required precautions to protect information, that is an Information Systems function**
    D. **Workstations will be used only for authorized business purposes related to the duties and responsibilities of associates**

HIPAA Review

15. A social engineer is a person who may try to talk you into giving them your log-in and password.

    A. **True**

    B. **False**

HIPAA Review

16. All St. Elizabeth computer systems are subject to a regular audit review including EPHI and Internet sites that you have accessed.

    A. **True**
    B. **False**

HIPAA Review

17. Which of the following is a good practice to prevent viruses and malicious software.

A. **Downloading internet software**
B. **Making sure not to by-pass or disable the anti-virus software on your computer**
C. **Installing personal soft or hardware**
D. **None of the above**

HIPAA Review

18. HIPAA violations by St. Elizabeth associates may result in disciplinary action up to and including termination from employment or volunteering.

    A. **True**

    B. **False**