HIPAA Education for Volunteers and Students

Objectives of Education
- Understand the basics of HIPAA Privacy and Security Rules
- Define Protected Health Information
- Understand the Notice of Privacy Practices
- Define Minimum Necessary
- Understand how HIPAA affects the day to day activities of volunteers
- Understand the risk of non-compliance
- Know who to contact for additional information

Health Insurance Portability and Accountability Act (HIPAA)

Purpose of HIPAA:
- Ensure continuation of health insurance benefits
- Reduce fraud and abuse in healthcare
- Improve the efficiency and effectiveness of the health care system
- Protect the privacy and security of all health information.

Protected Health Information
HIPAA applies to any healthcare information maintained either on paper or electronically, that could be used to individually identify a patient.
- Examples: Patient’s name, address, social security number, date of birth

HIPAA Privacy Rule
- It gives patients control over their health information.
- It sets boundaries on use and release of health records.
- It establishes appropriate safeguard requirements that health care providers must achieve to protect the privacy of health information.
- It holds violators accountable with civil and criminal penalties.

HIPAA Privacy General Rule
Healthcare providers may use and disclose protected health information (PHI) without a patient’s authorization for:
- **Treatment:** Sharing information with physicians, nursing homes, home health agencies
- **Payment:** Providing information to insurance companies.
- **Healthcare Operations:** Using patient information for St. Vincent Evansville business purposes (quality reviews, staff education, or to identify additional services needed in the community).
Minimum Necessary Standard

The “need to know” rule states protected health information should only be used or disclosed as necessary to perform your job duties.

Accessing patient information that you do not need to perform your job duties is a violation of St. Vincent Evansville HIPAA policies.

Examples: accessing information of co-workers, family members, friends, or your own information.

Recent Changes to HIPAA

Health Information Technology for Economic and Clinical Health (HITECH) strengthened privacy and security laws to protect health information from misuse as the health care sector increases use of information technology.

Changes include:
- Breach notification requirements
  - Examples of possible breaches include:
    - Faxing PHI to the incorrect number;
    - Mailing statements or a medical report to the incorrect patient;
    - An employee who is not authorized to access PHI looks through patient files in order to learn of a friend’s treatment.
- Increased penalties for violations
- Individual employees accountability for violations

Points to Remember

- Each employee/volunteer has a personal responsibility to understand and adhere to SVE policies and procedures to maintain confidentiality.
- HIPAA regulations require that we minimize the risk that protected health information (PHI) will be disclosed to individuals who do not have a need to know.
- All activities on SVE information systems are subject to monitoring. Users are responsible for all activities occurring on their user ids.
- Report possible/actual breaches such as faxing to the incorrect number, co-workers inappropriately accessing patient information, improper disposal of PHI.
- HIPAA Privacy & Security Officer, at 812-485-6550, privacyofficer@ascension.org

HIPAA Security

- All system activities are subject to monitoring.
- Employees are responsible for all activities initiated from their user ids.
- Passwords are the front line protection:
  - Select strong passwords:
    - Eight characters in length
    - Upper and lower case characters
    - Base ten digits (0–9)
    - Non-alphabetic characters (!, $, #)
    - Should not be based on personal information
  - Maintain the security of password:
    - Do not write down your password
    - Do not share your password

What can you do?

- Review St. Vincent Evansville HIPAA policies related to your duties.
- Speak in low tones and be aware of people in your surroundings. Do not discuss patients in elevators, hallways, cafeteria, or with friends or family.
- Do not share patient information on personal internet sites (Facebook, Myspace, etc).
- Select strong passwords.
- Log off computers when not in use and do not leave computers displaying PHI unattended.
- Verify publicity indicators.
- Verify fax numbers.
- Only access information that you need to know in order to perform your job duties.

HIPAA Resources

St. Vincent Evansville HIPAA Policies
- HIPAA Administrative Policy
- Protected Health Information Policy
- Uses and Disclosures of Protected Health Information for Facility Directory Purposes

St. Vincent Evansville Compliance, Risk & Accreditation Services Department at 812-485-6500
Office of Civil Rights website http://www.hhs.gov/ocr/privacy/