PRIVACY AND SECURITY TRAINING FOR VOLUNTEERS
Welcome to Patient Privacy and Security Training (HIPAA)

The requirements of the Health Information Portability and Accountability Act (HIPAA) are covered in this self-study module for UnityPoint Health volunteers.

HIPAA is an important federal law dealing with patient privacy and security of protected health information.

Please review this training module, complete the post-test you received during your Volunteer Services interview, and bring the completed test to your scheduled New Volunteer Orientation.

Thank You!
What is HIPAA?

• A Federal patient privacy law, enacted in 1996, called the Health Information Portability and Accountability Act or “HIPAA” which requires that we keep a patient’s protected health information confidential
• Protected Health Information is also called “PHI”
• PHI in an electronic form is called “ePHI”
• This includes a patient’s:
  - Personal information
  - Financial information
  - Medical information
“The Law” in Plain English

• HIPAA requires UnityPoint Health to protect PHI that it maintains or transmits
• Information related to a patient’s past, present or future physical and/or mental health or condition
• Includes at least one of the 18 personal identifiers listed on the next slide (Page 5)
• In any format: written, spoken, or electronic (including videos, photographs, and x-rays)
• PHI includes health information about individuals who have been deceased <50 years
• These rules apply every time you view, use, and share PHI
18 Personal Identifiers

- Names
- Postal address except State
- All elements of dates (i.e., birth, admission, death, discharge date)
- Telephone numbers
- Fax number
- Email addresses
- URL address
- IP address number
- Social security number
- Account numbers
- License/certificate numbers

- Medical record number
- Device identifiers and serial numbers
- Health plan beneficiary number
- Vehicle license plate and serial numbers
- Biometric identifiers (finger and voice prints)
- Full face photos and other comparable images
- Any other unique identifying number, code, or characteristic
Examples of Protected Health Information (PHI):

- Patient name, address, and age on a daily house census report
- Patient name and diagnosis in an electronic health record
- Patient name, phone number, and surgical procedure in a electronic patient scheduling system
- Patient name and medical record number stored in a diagnostic testing device such as EKG or ultrasound
- E-mail with patient name and medical record number
- Patient ID bracelets, IV bags and medication labels also contain protected patient health information
Why is Privacy Important?

• Patients expect and deserve privacy
  And..

• Federal and State laws require us to keep patient information private. There are fines and criminal penalties for organizations and individuals who violate these laws.
Who is Required to Follow HIPAA?

• The workforce of the covered entity is required to follow the HIPAA privacy regulations

• The workforce consists of:
  – All UnityPoint Health Staff
  – All Medical Staff
  – Students
  – **Volunteers**
  – Other business associates that are working with UnityPoint Health sharing patient information
Notice of Privacy Practice (NPP)

• The NPP informs patients how PHI will be used and disclosed for purposes of TPO. It must be presented at “time of first service” (usually for treatment).

  Treatment (T), Payment (P), Operations (O)

• TPO includes teaching, medical staff/peer review, legal, auditing, quality reviews, customer service, business management, and releases mandated by law.
It is appropriate to share patient information for Treatment, Payment, and Health Care Operations (TPO)... when required for your job.

Use only the *minimum necessary* information to perform your job duties.
Protecting Information

Protect verbal, written and electronic forms of information by:

– Following safe computing skills
– Following allowable use and disclosure of PHI
– Following proper disposal of PHI
– Following proper storage of PHI
– Reporting suspected privacy and security incidents
– Following UnityPoint Health Policies
Information Security means information must:

• *Be kept confidential* – the information is only accessible by authorized people and processes

• *Have integrity* – the information hasn’t been inappropriately changed or destroyed

• *Be available* – the information is ready when needed
Release of Information to Law Enforcement

- **Law Enforcement is not automatically entitled to PHI**
- State Law may require notification of Law Enforcement for certain injuries such as dog bites and gun shot wounds
- Most other PHI requests require Law Enforcement to sign HIPAA release of information forms and/or to provide a court order prior to the information being released
- Law Enforcement (if persistent) can be referred to:
  - Security
  - Nursing Administrator in Charge (NAC) on duty
  - Information Security Officer
  - Privacy Officer
Use of Social Media

- Do not share on social media any patient information acquired through your work at UPH, even if the information is public.
- Information obtained from your patient/provider relationship is confidential.
- Posting patient information without authorization is a violation of the patient’s right to privacy and confidentiality and a violation of federal law.
- Even if you think you’ve de-identified the information, people may be able to figure out who you are talking about.

**NOTE:** De-identification of PHI requires removal of all 18 PHI identifiers which includes “Any other unique identifying number, code, or characteristic” (e.g., photo of a wound; description of a patient’s condition).
- We discipline and terminate volunteers and employees for posting patient information to social media sites.
Identity Theft

• Identity theft is using the identifying information of another person.
• Identity theft can be in the form of financial identity theft or medical identity theft.
• Medical identity theft occurs when someone uses another person’s name or other parts of another person’s identity, such as insurance information or SSN, with or without the victim’s knowledge or consent, to obtain medical services.
• Medical identity theft also occurs when someone uses another person’s identity to obtain money by falsifying claims.
• The Identity Theft Program is in place to protect patient records and accounts maintained by the affiliates.
• Sharing an insurance card would be an example of medical identity theft. In addition to insurance fraud, this is a patient safety risk if two patient records become combined.
Audits of Electronic Medical Records

- Electronic Medical Records are routinely audited to check for possible HIPAA violations
- An automated audit software is used to look for inappropriate access such as:
  - Access of a family member’s record
  - Access of a patient in another department
  - Access of someone with the same address
  - Access of your own record (this is a policy violation)

Note: Inappropriate access by a volunteer can result in disciplinary action or even termination
Can I look up my own information in UPH electronic medical record systems?

**NO** - you may only look up information needed “to do your job”. You may access your personal information through the patient portal or by contacting HIM (Health Information Management Department).

Can I look up my family or coworkers records if they ask me to look something up for them?

**NO** - you may only look up information needed “to do your job”. Information concerning friends or acquaintances you see on the census or in the hospital is confidential. When and why an individual is in the hospital is a personal matter.
PLEASE REMEMBER-

‘What you see here, What you say here, When you leave here, Must stay here!’
Common Privacy Breaches

- Talking in public areas, talking too loudly, or talking to the wrong person
- Lost/stolen or improperly disposed paper documents, films, notebooks, medication bottles
- Lost/stolen unencrypted laptops, tablets, cell phones, media devices (video and audio recordings)
- Lost/stolen unencrypted zip disks, CDs, flash drives, memory sticks
- Hacking of unprotected computer systems
- Email or faxes sent to the wrong address, wrong person, or wrong number
- Users not logging out of computer systems, allowing others to access their computer or system
You Must Report.....

• UnityPoint Health policies require you to report a privacy or security breach. Contact any of the following:
  – Privacy Officer
  – Information Security Officer
  – Compliance Helpline @ 1-800-548-8778 (anonymous)
  – Your Supervisor

• Our policies prohibit UnityPoint Health from retaliating against you or taking disciplinary action in any way because you report a privacy or security breach

• UnityPoint Health’s policies and the law also protect you for engaging in certain good faith compliance activities, such as participating in government investigations
UnityPoint Health is required to implement reasonable security measures to protect electronic Protected Health Information (ePHI)

- Technical Security
- Physical Security and
- Administrative Security
**Technical Security Measures**

- Unique UserIDs/Logins
- Emergency procedures for access to ePHI
- Authentication (passwords, fingerprints)
- Single Sign-On
- Automatic Logoffs
- Encryption of ePHI
- Controls to ensure ePHI in transit over a network is not improperly modified or destroyed
- Audit controls
**Physical Security Measures**

- Back-up plans for downtime
- Facility security plans
- Door access for secure areas such as server rooms
- Maintenance records for facilities
- Privacy screens and screen savers
- Dispose PHI in locked shredding bins – don’t throw PHI into the regular trash containers
- Procedures for disposal and re-use of hard drives, DVD’s, flash drives, etc.
- Tracking of computers
- Back-up procedures for record access
Administrative Security Measures

• Thorough inventory of applications and systems containing ePHI
• Review of audit logs, access reports and security incident tracking reports
• HR policies addressing violation of HIPAA security policies and procedures
• Authorization/supervision of workforce clearance procedures
• Plans for access to and recovery of ePHI during a disaster (e.g., tornado, flood, fire) or other reasonably anticipated emergency events
• User access and termination procedures
• Education for users on security issues
• Log-in monitoring procedures
• Password management procedures and training
Keep Patient Information Secure

• Beware of computer viruses!
• Viruses can give outside people access to our patient information
• To prevent a virus from getting on your computer, follow these tips:
  – Never open a link from an unknown sender or in an email that looks suspicious
  – Contact the IT service desk to report any suspicious emails
Would you hand the keys to your house to a stranger?

Don’t respond to an e-mail request for your login and password, ever.
**Phishing and Spear Phishing**

They are essentially trick emails, that convince a person to open an attachment or click a link that leads to an infection with malware. This malware can be devastating. It can literally lead to your entire hard drive or corporate drives from being silently encrypted. The criminals then require a ransom to be paid to get the data unencrypted. This is called Ransom Ware. They can also ask for your login credentials, log your computer key strokes, etc.

- This is an example of what a phishing scam in an email message might look like
  - Subject: Your password will expire soon
    Date: January 19, 2016
  - <BAD LINK: Click here to proceed with your Email update>
UserID’s/Login Security

• You are responsible for all actions taken under your UserID!
• Never share your username and password with anyone!
• If you think someone has used your UserID, or tried to use it, you must call the IT Service Center immediately to change it.

Signs to look for:
  – The system you are signing into shows your last log-in occurred when you were on vacation
  – Your password no longer works (some systems will lock out users after three failed sign-in attempts)
**Passwords**

- You will be required to enter a password to access ePHI
- You are responsible for maintaining the confidentiality of your password! If you suspect an unauthorized disclosure of your password, notify the IT Service Center immediately.
- You should not write down your password and store it in a location where another person might discover it (e.g., stuck to monitor, under keyboard, or in a desk drawer). Store it in your purse or wallet instead.
- Passwords are changed every 90-150 days.
Examples of Good Passwords

- Passwords must contain a minimum of 8 characters with upper & lower case letters and numbers.
- Passwords should not consist of repeating characters (11111111 or abababab), UserIDs, birth dates, employee or social security number, telephone numbers, common sequence characters (12345678), common words found in the dictionary, or names of a spouse, parent, child, or pet.
- Instead, use:
  - 2 small words joined with a special character or number
    Example: Dog#house1, dog8House
  - Words with numbers inserted in place of vowels
    Example: D9gh97s3
  - The first letters of a sentence or phrase
    Example: Il2stMoA (I love to shop the Mall of America)
• Don’t answer any security questions or provide any personal information to *anyone* via the phone – unless **YOU** have initiated the phone call for your own known purposes.

• In other words, if you need a password reset and call your service provider to reset your password, they will legitimately ask you security questions (last four digits of your SSN, or your PIN or whatever necessary to validate your identity via the phone).

*If you didn’t initiate the call – it is a scam!*
• You are responsible for logging off or locking your workstation (Windows key + L) before leaving it unattended.

• Screen savers and pre-set auto log-off functions are used to protect ePHI on unattended workstations.

• You are responsible for securing your laptops, tablets, and any removable media when you leave your workspace (such as locking a laptop in a car trunk when leaving unattended in a vehicle).
PRACTICAL TIPS FOR HIPAA

ALWAYS, ALWAYS, ALWAYS...

- Protect verbal, written and electronic forms of PHI
- Only access PHI to do your job
- Dispose of PHI properly
- Use the minimum necessary to perform your job
- Protect your login and password
- Report any potential HIPAA violations immediately
MORE PRACTICAL TIPS

AVOID...

• Sharing information with co-workers who do not have a “need to know”
• Discussing patient information in public places (elevators, Giftshop, cafeteria, or when using Vocera, etc.)
• Accessing your own or others PHI when not needed to perform your job
• Posting PHI on social media
• Sharing your password with others
• Introducing viruses or malware into the system
UPH hopes its compliance steps will be very effective.

As an organization, UnityPoint Health faces potential civil fines for violations of the HIPAA privacy and security rules. Fines may be $50,000 per violation with an annual maximum of $1.5 million.

Volunteers and employees also face criminal penalties for violations of HIPAA. The severity of the penalty depends on the conduct.

- For example, if an volunteer intentionally obtains PHI about a patient by using a false identity, the worker could be fined up to $100,000 and get 5 years in jail.
- If PHI is improperly used or shared for commercial advantage, personal gain, or malicious harm the worker may be fined up to $250,000 and get 10 years in jail.

Violations of HIPAA policies and procedures may result in disciplinary action up to and including termination.

UPH’s corrective discipline policy is available through the Volunteer Services Office or on the Intranet.
If you have questions regarding HIPAA compliance:

Contact any of the following-

- Your Supervisor/Manager
- UPH – Meriter Privacy Officer
- UPH – Meriter Information Security Officer
- Volunteer Services Office
- Compliance Helpline 1-800-548-8778 (anonymous)

Feel free to review the preceding slides until you are confident about your knowledge of the material presented.

So, now you are ready to complete the Privacy and Security post-test that you received during your interview. Bring the completed test with you to your scheduled New Volunteer Orientation.

Thank You!