HIPAA – Health Insurance Portability and Accountability Act of 1996

WHY DO YOU NEED TO KNOW ABOUT HIPAA?

Simply by being in the medical center, you will encounter confidential information. You need to be prepared to handle those situations appropriately because there are penalties that could impact YOU and VUMC if the confidentiality rules are broken. VUMC has its own set of rules that incorporate Federal regulations. Disciplinary/corrective action ranges from training/counseling to termination. Everyone who has access to our patients or protected health information (PHI) is required to understand our privacy and information security policies and abide by them. The complete policies and other details can be found on the HIPAA web site: www.mc.vanderbilt.edu/HIPAA

PROTECTED HEALTH INFORMATION (PHI)

PHI is any information related to health conditions or services that can be linked back to an individual patient. PHI can be in any form: written, electronic or verbal. This means that essentially all information linked to a patient at VUMC is PHI. **Even the fact that a patient has received care at VUMC is protected by our policy *and* federal regulations**.

KEY QUESTIONS TO ASK YOURSELF ABOUT HOW YOU ARE USING PHI

1. **Are you authorized to access information about this patient?** You should only access and use PHI as required to do your job or when specifically authorized by the patient.
2. **What information can be shared?** PHI should only be shared on a need-to-know basis (i.e. direct patient care, risk management, quality review).
3. **Did I ask the patient if it is okay to discuss their health Information?** Never assume it is okay to discuss patient information in front of visitors and family members. Always ask is it okay before doing so.
4. **Where and How are you sharing information?** Because care is often coordinated in semi-public areas in the Medical Center, it is essential that everyone be aware of their surroundings when using and sharing patient information. Be careful to prevent unauthorized persons from overhearing or overseeing confidential information. Don't talk in halls or elevators. Also, take care when faxing, handing, emailing, and disposing of PHI.

SECURITY

Below are some key security concepts that you should keep in mind while working at VUMC.

1. **Passwords** – Never share your password or use someone else's password. Create a hard to guess password that includes numbers, letters, and special characters (where the system allows).
2. **Logging off** – If you need to walk away from a computer, you must Log off **OR** Lock the screen.
3. **Mobile Devices (laptops, PDAs, and text pagers)** – These devices should always be password protected to prevent unauthorized individuals from accessing them in case they are stolen or left somewhere unattended.
4. **Email –** Do not forward your VUMC email to your personal email address.
5. **Cloud-Based Computing and Data Storage –** Consumer available Cloud based computing and data storage services (such as Box, DropBox, SkyDrive, and GoogleDocs) should **not** be used to store, collect, or share Vanderbilt University Medical Center (VUMC) patient or other confidential information unless the cloud-based service has been approved and confirmed via a Vanderbilt contract and a HIPAA compliant Business Associate Agreement.

HAVE QUESTIONS? If you have a question your VUMC contact is unable to address, call the Privacy Office at (615) 936-3594. You may also visit our website at: http://www.mc.vanderbilt.edu/HIPAA. If you witness a violation of our privacy policies, you are encouraged to contact the Privacy Office, Help Desk, Compliance Reporting Line, or your manager.