HIPAA Privacy & Security: Our Values and Ethics at Work

HIPAA (Health Insurance Portability and Accountability Act) is a Federal regulation imposed on health care organizations including hospitals, home health agencies, physician offices, nursing homes, other providers, health plans and clearinghouses.

HIPAA Privacy Rule: Gives patients a right to access their medical records and restrict (in some ways) who may access their health information. Requires organizations to train its workforce and to take measures to safeguard patient information in every form. Provides penalties for individuals and organizations who fail to keep patient information confidential. Criminal penalties under HIPAA: maximum of 10 years in jail and a $250,000 fine for serious offenses. Civil penalties under HIPAA: maximum fine of $25,000 per violation.

HIPAA Security Rule: Pertains to electronic patient information and requires physical, technical and administrative safeguards.

Protected Health Information (PHI): PHI is any patient information which indentifies a patient directly or indirectly. PHI in any form (written, faxes, electronic, photographs/images, conversations, labels, monitor strips) must be protected.

HIPAA Privacy Official and HIPAA Security Official: The Privacy Officer shall oversee all ongoing activities related to the development, implementation and maintenance of the practice/organization's privacy policies in accordance with applicable federal and state laws. The Security Officer is responsible for the ongoing management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all organizational healthcare information systems. Please consult your volunteer office for names and phone numbers of the HIPAA Privacy Officer and the HIPAA Security Officer.

Privacy and Security Tips:

- Do not look at PHI unless you need to know the information to do your job.
- Use the minimum amount of PHI necessary to perform your job duties.
- Do not use your work access privileges to access, view or print your own PHI or the PHI of your spouse, children, other family, friends or coworkers.
- Be conscious of who else may be listening when speaking with patients or family members.
- Lower your voice when appropriate or move to a more private location.
- Dispose of PHI by shredding it or placing it in a locked confidential storage container. Do not place PHI in the regular trash.
- Before giving out paperwork, make sure each page is for the correct patient.
- Patients (including you) should go to the Health Information Management (HIM) department to complete the required paperwork to obtain copies of their PHI. HIM employees will verify identity and legal rights to the information and release it as appropriate.
- Do not discuss what you overhear about a patient or share information gained in

the course of work with your family, coworkers, or friends.

- Do not discuss PHI with others who do not need the information to perform job duties such as those you encounter at Walmart, church, or grocery stores.
- Do not discuss patients in public areas such as elevators, hallways, or cafeterias, where individuals outside the healthcare team may hear you.
- Do not leave an individual without identification in a confidential or secure area. Offer assistance and ask for identification if necessary.
- Do not leave patient records lying around where visitors or other unauthorized persons may view them. Keep them secure.
- Keep PHI in folders, turn it face down or use a cover page.
- Remove PHI from printers, fax and copy machines in a timely manner.
- Do not post or write down your passwords. Never share your password. Make your password something you can remember but difficult for others to guess. Do not include personal information others may know about you in your password (name, date of birth, spouse or children's names, pet names).
- Log out of patient information systems when you leave your work area.
- Turn patient information monitor screens away from public view.
- Verify you have entered the correct fax number before faxing PHI.
- Use a fax cover sheet with appropriate confidentiality language.
- Be mindful of your location when discussing PHI on a cell phone.
- Avoid using speakerphones when discussing PHI.
- Be careful about how much PHI you leave on home answering machines.
- Keep laptops and other mobile devices secure at all times.
- Always wear your identification/name badge where it is visible to others.
- PHI on labels must be removed and placed in a locked confidential storage bin, or marked through with a black permanent marker or placed in hazardous waste container if appropriate.
- If you are not involved in the care of the patient or the welfare of the family, remove yourself from the area of confidential patient discussions.
- After asking their permission, put phone calls on hold to prevent overhearing background conversations about other patients.
- Knock and pause before entering the patient's room.
- Ask visitors to leave the room if the patient would like them to do so before discussing PHI.
- Direct media inquiries to Public Relations or Administration.
- Report potential violations to your Volunteer Services office, Privacy Officer or Security Officer.

Notice of Privacy Practices (NPP): Provided during the patient's first visit, posted in the facility, and on the website. Outlines: how we may use and disclose PHI, rights regarding their PHI and how to access it, how to file a complaint or opt out of the facility directory, and how to request a list of those who have received their PHI (Accounting of Disclosures), amendments, alternative means of communication (Confidential Communications), and restrictions.

TPO (Treatment, Payment and Operations): HIPAA permits us to share PHI for treatment, payment or operations (coding, billing, quality review, risk, etc.) without authorization from the patient.

Authorization: WVU Medicine must obtain a signed and dated authorization form from the patient before using or sharing PHI for reasons other than TPO unless the use or disclosure is mandated by law.

Marketing: In most cases, we may not use or disclose PHI to market or film or photograph a patient for marketing purposes without obtaining a valid signed and dated authorization form from the patient. If an outside entity is involved in filming, photographing or interviewing a patient, please work with the Public Relations department. Certain forms must be signed by the patient and by those filming, photographing, or interviewing the patient.

Legal Personal Representatives: Persons having the authority (under federal and state laws) such as Durable Power of Attorney with a healthcare designation or Health Care Surrogate or Court Order to act on behalf of a patient in making healthcare decisions have the same rights to access the patient's information unless the involvement of the personal representative would put the patient at risk.

Legal Personal Representatives for Minors: Parents, guardians, and others who have authority (under federal and state laws) to act on behalf of a minor in making healthcare decisions also may have access to the minor's health information as his/her personal representative unless the minor is emancipated.

Discussing PHI with a Patient's Friends and Family: HIPAA permits hospitals to share *information that is directly relevant to the level of involvement* of a family member, friend, or other person identified by a patient, in the patient's care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, you may discuss this information with the family or other persons if the patient agrees or, when given the opportunity, does not object. You may also share relevant information with the family and other persons if you can reasonable infer, based on professional judgment that the patient does not object. Even when the patient is not present or it is impracticable because of emergency circumstances or the patient's incapacity for us to ask the patient about discussing his/her care or payment with a family member or other person, you may share this information with the person when, in exercising professional judgment, you determine that doing so would be in the best interest of the patient. You may also disclose PHI as necessary to obtain payment for services provided. You may contact persons who are involved with the patient's care and payment for services other than the individual as necessary to obtain payment for health care services. You are required to reasonably limit the amount of information disclosed to the minimum necessary to process payment.

Facility Directory: A patient has the right to *opt out* of the facility directory. Check the directory before responding to any inquiries about a patient. If the patient has agreed to be in the directory, release only location and general condition (fair, critical, etc.). If the patient has opted out of the directory, advise the caller or individual present that you have no information on the individual requested. The internal process used by WVU Medicine to identify patients who have opted out of the directory is the word “yes” listed beside the patient’s name.

Access is monitored: Electronic access to PHI is monitored. Inappropriate access or sharing of PHI results in disciplinary action up to and including termination.

Breach Notifications: Hospitals must notify patients within 60 days if their unsecured patient information was acquired, accessed, used or disclosed inappropriately. The notice must describe what happened and what the organizations is doing to investigate the breach, how similar breaches will be prevented in the future, steps individuals can take to protect themselves and contact information. Patients will be able to sue and may be able to receive compensation for breaches. Breach investigations and notifications will be handled by the Privacy Officer and the Privacy Coordinators.

What is Your Responsibility?

If you suspect a patient’s privacy has been violated, or if a patient alleges his/he patient information has been accessed, used or disclosed inappropriately, immediately call the Privacy Officer.