Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule and Compliance

The HIPAA Privacy Rule (45 CFR Part 160 and Part 164) establishes national standards to protect individual's medical records and other personal health information. The Privacy Rule applies to health plans, health care clearinghouses, and health care providers that conduct health care transactions electronically.

The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

The Privacy Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Students are required to adhere to the Health Insurance Portability and Accountability Act (HIPAA) during all rotations, volunteer experience, and research. Violations of HIPAA and patient confidentiality will result in removal from rotation, a failing grade for that rotation, and may result in civil or criminal penalties as prescribed by current HIPAA Privacy Rule regulations. Additionally, California law provides for severe civil and criminal penalties for violating patient confidentiality.

What patient information must we protect?

All information about an individual who is a patient of a health care service is private or confidential. The information may be written on paper, saved on a computer or spoken. HIPAA refers to this information as Protected Health Information (PHI).

PHI includes:

A person's name, address, phone numbers, e-mail address, age, birth date, social security number

Medical records including the reason for seeking health care, diagnosis, prescribed treatment and medications, x-rays, lab work, test results

Billing records including claim information, referral authorizations, benefits explanations, research records. If you have access to any of this information—including the simplest fact that a person received health services—and reveal it to someone who does not need to know it, you have broken the law and compromised a person's confidentiality.

What is not considered PHI?

Health information is not protected health information if it is de-identified. De-identified information may be used without restriction and without patient authorization. The de-identification standard provides two methods for which health information can be designated as de-identified. The first method requires the removal of all 18 identifying data elements listed in the regulations. If the resulting information cannot be used to identify the individual, then it is no longer PHI. The second method requires an expert to document their determination that the information is not individually identifiable ("Expert Determination").

How does HIPAA affect you while on internships, clinical rotations, volunteer experiences, and research?

As part of your experiences with access to patient data you must protect the privacy of PHI.

When can you use PHI?

You can only access and use PHI to fulfill your educational responsibilities while performing your internship, IPPE/APPE, volunteer, clinical rotation experience, or research. You should, at all times, protect a person's information as if it were your own information.

You may look at a person's PHI only if you need it as part of your internship, clinical rotation, volunteer experience, or research; use a person's PHI only if you need it to complete your responsibilities on your internship, clinical rotation, or pharmacy practice experience(s); give a person's PHI to others when it is necessary for them to do their jobs, and/or talk to others about a person's PHI only if it is necessary to the internship, clinical rotation, volunteer experience, or research.

Need to Know?

Use common sense in making decisions about whether you need to see or share PHI to perform your task. Ask yourself,
"Do I need to know this to be effective in the pharmacy practice experience, volunteer experience, clinical rotation, or research I am doing?"
If you do not, do not access the information. It is none of your business! But if it is your business, you have nothing to worry about.

WHAT ELSE SHOULD I BE THINKING ABOUT TO PROTECT PRIVACY OF PHI?

Strong computer security practices are protective of private information. These are some best practices to implement:

Use common sense when receiving attachments from strangers. Don't open a file unless you have reason to have expected to receive one.

Pay attention to "cries for help" from your computer. If hackers have gained access, you might notice the disk drives chattering when you aren't asking the computer to do anything. Subtle changes to your desktop might suggest someone is running "remote control" software against you.

Clear off disk drives before disposal of computers. Use a "disk wipe" program or a low-level format.

Use a screen saver that locks your desktop when you are away from your desk.

For more information and resources regarding HIPAA, please click here.