Please read the Sanford Health HIPAA Information:

Health Insurance Portability & Accountability Act

HIPAA: National Privacy Law

The Health Insurance Portability and Accountability Act of 1996 makes it illegal to violate patient confidentiality. The Privacy Rule of 2003 and the Security Rule of 2005 were added to the original HIPAA law. These laws apply to:

- Sanford Staff
- Job shadow (observation) people
- Business associates of Sanford Health

The Privacy and Security Rules added:

- Grants individuals certain rights over their health information
- Sets rules and limits on who can look at and receive health information
- All forms of Protected health information (PHI), whether electronic, written, or oral
- Technical and physical items such as computer passwords

Patient privacy is our highest priority. When discussing what you have seen or heard with the staff member you are shadowing, do so in a private area so information is not overhead. Outside of your job shadow, you will **not** discuss with anyone:

- Personal details relating to a patient
- Patient medical history
- Care-related discussions about patients in public areas where conversations may be overheard
- Anything you may see in the medical record
- Any patients, visitors, or relatives you may see

You are not allowed to ask to see your own medical information. Maintaining the security of confidential information is your duty and responsibility. **What you hear and see stays at Sanford**.

Knowledge Check

You are with a team of people caring for a patient. Can you ask questions about the patient?

Yes, you can ask questions during your job shadow time in an area where you cannot be overhead.

You hear information about a family friend. Can you talk with your family members what you hear?

No, this information is confidential and protected by state and federal privacy laws. You may not discuss any private information with anyone not directly involved in the care of the patient.

You are talking with the staff member hallway about the treatment plan for the patient. A visitor who is passing by overhears you. Did you violate HIPAA?

No, **but** you should avoid discussions in public places whenever possible. This is not a violation of the law if you are being reasonably careful. Do not talk about patient information where visitors or other people can hear.

Sanford Health is responsible to:

- Educate you about these rules
- Monitor rules are followed
- Act on situations when someone violates HIPAA
    - No Exceptions
    - No Excuses
        - **This includes stating you are a student and did not know what HIPAA was**.

Important Terms

Protected health information (PHI) is information specific to a patient and must be kept confidential. This includes:

- Name
- Phone number
- Social Security number
- Address
- Condition-why they are in the hospital or other medical information
- Date of admission

Patient signature or approval is not required for their information to be shared for education. The staff member you are with will ask verbal permission for you to enter a patient's room. Patients have the right to refuse a student.

What Happens if HIPAA is violated:

- Civil fines range from $100 to $50,000 per violation depending on the violator's intent, up to $1.5 million per year for each violation
- Criminal punishments include up to $50,000 and one year in prison for knowing violations of the law, up to $100,000 and five years in prison for misusing PHI under false pretenses, and up to $250,000 and 10 years in prison for misusing PHI maliciously for monetary gain.

Patients' Rights to their Medical Record

Patients can request:

- Amendments (changes) to their records
    - Health care facilities may allow or refuse to make the changes based on the input of the physician. For example,
        - If a patient wants to remove information regarding smoking because they quit last week, the provider may say this history of smoking and important information to keep in the record.
- Restriction of uses and disclosures
    - Patients can ask that their medical information is not shared with specific groups or persons. The health care provider does not have to agree to the request. If providers agree, they cannot change their mind. For example,
        - The health care provider agrees to a request not to send information to the patient's insurance company. The patient is paying for the service with cash, not going through insurance.
- Access their own PHI
    - Health care providers must give patients access to their records. Sanford encourages providers review the material with the patient to explain the information and ask questions.
- Receive an accounting of disclosures
    - Patients may review the list of places their records have been sent to (disclosed). Items that will not appear on the list are:
        - Payment inquiry

(other than things sent because of treatment, payment and operations).

- Request confidential communications
    - Patients can restrict how information is shared. For example:
        - Patients may ask that reports are sent to their office, not their home.

Knowledge Check

When the nurse is reviewing the patient's allergies, the patient states they are not allergic to penicillin. She asks the nurse to change that information since the information is not correct. The nurse submits the request, and the provider approves the change. The appropriate person in medical records makes the change. Can this happen?

Yes, patient rights allow the patient to request changes. Only those authorized to make changes to the legal record may do so.

Mr. J is furious that he is getting advertisements from a drug company ever since he was diagnosed with cancer. He wants to know if the hospital told the company of his diagnosis. Can he be shown an accounting of all the places his PHI was disclosed too?

Yes, the hospital can show the patient the places his PHI was sent to.

Your patient requests for you to print a copy of their medical record to have on file at home. Can you do this?

No, patients are not automatically given their medical record. The medical record is owned by the facility. Patients must request their medical record through the release of information (ROI) process. Patients can access their medical record through the My Chart Sanford App at any time.

A patient comes into the emergency department drunk, following an accident. The police arrive and request to read the patient's record. The staff refuses to let them read the record. Is this right?

Yes, law enforcement is not to be given any information. There is specific laws Sanford must follow. The staff member will use the chain of command in these situations.

You are a patient at the same health care facility you are shadowing. You want to review your medical record or your family members. You can ask a staff member to show them to you on the computer. Is this, okay?

No, students are not allowed to access, inspect, or copy their own medical information or any family members. They must request this information through the ROI process.

A patient is admitted in serious condition and has asked that we do not list them as a patient in our system. This means no information can be shared with anyone. When the patient's daughter calls asking to see if her mom is here, the staff member says "I am sorry. Either your mother is not a patient in our hospital or has requested not to be listed in our directory." Is this the right answer?

Yes, patients can choose not to be listed in our directory (no location, no information). Patients can request:

- No information be given
- Name and room number given
- General information given about their condition

All information related to any patient is considered confidential.

Patient Identifiers

HIPAA requires you cannot use PHI for:

- Assignments
- Conversations with teachers and other students
- Any other activity that may occur.

There are 18 specific PHI identifiers listed in the Privacy Rule that cannot be talked about or seen. These include:

- Names
- Certificate/license numbers
- Geographic: address, city, county, precinct, zip, etc.
- Vehicle identifiers; serial numbers & license plates
- Dates such as admission or discharge, birth or death
- Device identifiers & serial numbers
- Telephone numbers
- Web URLs
- FAX numbers
- Internet protocol addresses
- Electronic mail addresses
- Biometric identifiers (finger and voice prints)
- Social Security numbers
- Full face photos & comparable images
- Medical record numbers
- Any unique identifying number, characteristic, code
- Health plan beneficiary numbers
- Account numbers

Knowledge Check

When discussing your experience with your teacher you can say "I cannot tell you who this person is, but she works at Sears in the electronics department." Is this correct?

No, you cannot give any information that could possibly identify the patient.

Sharing Information

As part of your education, you may need to share your experience with health care facility staff, teachers, or other students. The sharing of patient data in verbal, written, and electronic formats is only appropriate when you do so as a part of your job shadowing experience. Remember to not use PHI identifiers.

Knowledge Check

If you need to fill out a form to turn into your teacher, you can write down your experience if you do not use any of the identifiers listed above.

Yes, be sure your paperwork does not include any patient identifiers. The staff member you are shadowing can help you.

You see someone from your hometown walking down the hall in a patient gown. You want to tell your mom. Is this, okay?

No, you would be in violation of the privacy rule.

You watched a surgery today and the patient had a cool tattoo. You want to tell your friends about the tattoo. Is this, okay?

No, if you share any patient information (unique characteristic), like the tattoo, with your friends you have broken the Privacy Rule. Remember, sharing any patient information is only appropriate when you do so as part of your training with the staff member you are with.

You can ask the staff member you are shadowing at the hospital cafeteria about something you saw in a medical record. Is this the correct setting?

No, confidential information may only be shared with staff in a private area. **Do Not** discuss private information in the cafeteria, elevator, stairwell, waiting room, meeting room, or public areas.

The HIPAA Security Rule

The Security rule is primarily an e-rule, which means that electronic protected health information must be secured from access by the wrong people. Every health care worker and student must know the following E-HIPAA rules:

- Password management
- Access controls
- Monitoring
- Viruses and malicious software

You will not get a password to the computer charting system or any entry into rooms that have PHI. Do not ask staff for their passwords or codes to obtain PHI. Staff members are responsible to get their passwords and codes protected and safe.

Access Controls

Only the people who need to know PHI for healthcare and billing reasons should have access. Sanford educates and puts measures in place to protect health information. These include:

- Staff who have passwords will not share them with anyone or write them down where they can be seen.
- Computer screens will go log out after a certain amount of time. Staff are educated when stepping away from the computer to always sign off.

- Keep computer monitors from facing the public so information cannot be seen.

Remember if you see PHI during your job shadow experience, you cannot share that information with anyone.

Security to Control Access to PHI

PHI is also locked in rooms. Physical security devices can be locks, keypunch pads, or electronic locks to that need a badge to enter. Never put PHI on:

- Removable media or devices such as:
    - Computer flash drives
    - CDs
- Any electronic device such as cellphones, tablets, or laptops

When you delete PHI that has been saved to any external device, it does **not** completely go away.

You will not have access to Sanford's email system. You cannot type any patient's PHI in your personal email.

Monitoring Computer Use

The Security Rule states that health care facilities must monitor computers used throughout their computer network. The law requires that facilities monitor:

- Who is on the Internet
- Who is going in and out of the main computer room
- Who entered information into the clinical computer system
- Promptly remove all passwords and access when no longer needed
- Record when someone:
    - Enters the system
    - Reads and clicks in the EMR
    - Charts information
    - Leaves the system

Knowledge Check

Is it okay to look up inappropriate content on the hospital internet?

No, this is the hospital property. The hospital monitors internet and device usage.

Is it okay to download information onto your USB for your shadow assignment for school?

No, this is the hospital property. You can write down information that is not PHI for your school assignment. You cannot take, download, or send any information that belongs to the hospital.

You can be held **legally responsible** for violating the computer monitoring use policy.

Protection Against Viruses and Malicious Software

Firewalls are protections to keep viruses out of the system. Virus scanning software activated in the system keeps unknown software out. This software will not be able to stop all virus activity. New viruses are created frequently and may not be recognized as viruses. This may happen when electronic devices are used that do have the facility approved software. The personal devices may connect to the Sanford system and a virus from the personal device may enter the secured Sanford system.

How You can Help Protect Against Viruses While Job Shadowing

While you are in Sanford it is important to keep the system safe. You can help. Here is list of things to not do to protect the system. **Do not**:

- Go into email accounts like Hotmail
- Open unknown attachments or unfamiliar emails that come into any computer.
- Load software on computers, including PDA (personal data assistant) docking stations
- Open unknown computer programs
- Bring your personal laptop or any personal devices with you
- Download electronic music files
- Add storage devices
    - Zip drive
    - Flash Drive
    - DVD writers