HIPAA which stands for Health Insurance Portability and Accountability Act, is a broad law that
deals with a variety of issues. An important part of the law discusses patient privacy and
confidentiality. Under HIPAA’s privacy and security sections, it is illegal to release health
information to inappropriate parties or to fail to adequately protect health information. The new
privacy and security regulations will impact any employee or hospital representative who comes
in contact with a patient or comes in contact with patient health information. Our organization is
committed to establishing and observing the highest standards of ethical conduct in business,
preserving patient confidentiality, and ensuring proper coding and billing practices. Our
Compliance program also promotes detection and prevention of violations of federal, state, local
laws and regulation.

H - HEALTH

I - INSURANCE

P - PORTABILITY and

A - ACCOUNTABILITY

A - ACT
PROTECTION STRATEGIES FOR PATIENT PRIVACY

Whether patients are in the hospital, x-ray, ICC or the physician’s office, patients receiving medical care expect and deserve privacy. Patients expect to be physically separated from other patients and employees when they discuss their personal medical condition with their doctors and nurses, and patients assume that their private health information will not be shared with other employees.

Norton Healthcare is committed to giving patients privacy. While at Norton Healthcare, you will see many ways patient privacy is guarded and protected.

- Patient care or discussion about patient care should be kept private by closing room doors or drawing privacy curtains and conducting discussions so that others may not overhear them.
- Patient medical records should not be left where others can see or access them. All test results and the outcome of procedures must be kept private.
- Patient financial information discussed during registration should also be conducted in a private area, and any information taken should be kept confidential. This feeling of privacy is essential to the Norton Healthcare’s mission. As you perform your job, you need to protect patient privacy.
- As part of your duties, remember that you don’t want to interfere with patient privacy or jeopardize the confidentiality of patient health information.
**STEPS TO PROTECTING PATIENT PRIVACY**

The common sense steps to protecting patient privacy have been the hallmark of Norton Healthcare.

- Employees should knock on a door and ask to enter before entering a patient’s room.
- Patient records must be locked away and/or out of public areas. If nursing, housekeeping and engineering personnel find patient records unattended, return them to the nursing supervisor.
- If you need to page family members, the page should not include information that can allow others to identify the patient’s doctor, the department in which he or she is being treated, or any information about why he or she is on the premises.
- If you find that you are overhearing someone else discuss patient care, remind that individual of the Norton’s policy and let him or her know that they can be over head.

**DISCIPLINARY ACTION AND PENALITIES**

The potential penalty from breaching privacy and security issues at Norton Healthcare is the possibility of termination. The misuse or unauthorized disclosure of confidential patient health information, including unauthorized access or the inappropriate copying of patient data may result in termination. In addition, divulging or allowing others to use you confidential password; or obtaining or using the confidential password of another employee may result in termination.

The U.S. Department of Health and Human Services (DHHS) will enforce HIPAA. Breaking HIPAA’s privacy or security rules can mean either a civil or criminal penalty.
HOW IS PROTECTED HEALTH INFORMATION (PHI) USED?

Norton Healthcare collects PHI so that we can take care of patients. However, your facility and its workforce can use it only in limited ways.

- Doctors, nurses, therapists, dietitians, and others use information about patients to determine what services the patient requires.
- The billing department uses confidential information to be able to bill patients or their insurance companies for services they received.
- Physicians and case manager’s review confidential PHI to make sure patients are getting quality care.

Ask yourself before looking at any PHI:

- Do I need this patient information in order to do my job and provide quality patient care?
- What is the least amount of patient information I need to perform my job?

*Remember, the requirement to use or share only the “minimum necessary” information is covered in the HIPAA privacy rule.*
**CAN I SEE PHI?**

Each and every one of us at Norton Healthcare contributes to the quality of patient care. However, that doesn’t mean everyone needs to see protect health information about patients.

- Many positions have no access to patient information, either in the computer or in paper form. Why, because they don’t need to know the information. A phrase to remember: Need to know.

- Patient health information contained on whiteboards boards is used for providing care to patients. In general, it is recorded in places where the public can not see it. But some employees may work in areas where this information is visible. This information is confidential. That means that it is not to be used by you in any way or told to anyone, including coworkers, other patients, patient visitors, or anyone else who may ask you about it.
HEAR FROM YOUR CO-WORKERS

Employees identified these common breaches in privacy and security issues.

- What about the patients that ask, “my roommate seems awfully sick. What are they here for”?
- One employee says, we breach patient privacy when a co-worker is having a test or procedures done at the facility for which they work, and other co-workers look up the results of the test or procedure. However well meaning, this is WRONG.
- Another employee said, during smoke breaks, I overhear nursing staff telling housekeeping and engineering staff about the specific patients. They even mention patient’s names while there are visitors and families of patient’s smoking.
- One employee notes, I have seen breach of privacy when I see security personnel and ancillary staff talk about patients of families of patients in public places such as an elevator or cafeteria.
- One employee has noticed that OR staff and doctors throw away the typed OR schedule without shredding or placing in the shredding bin. The OR schedule includes the patient’s name and the surgical procedure.

Norton Healthcare is committed to protecting patient privacy and patient confidentiality. When you fail to protect patient information and patient records by not following your organization’s privacy and security policies, it reflects on your ability to perform your job.
CONCLUSION

In the course of doing your job, you may also find that patients speak to you about their condition. While there’s nothing wrong with this, you must remember that they trust you to keep that information confidential and you must not pass it on.

In an organization the size and complexity of Norton Healthcare, privacy and security issues will arise from time to time. We can’t design a system that will always be problem-free, but we can have policies and procedures designed to prevent privacy and security breaches. What is most important is not that we may have problems but how we can create and implement privacy and security processes to eliminate or minimize these problems.

If you become aware of a situation or process you think might violate patient privacy and confidentiality, you can notify your supervisor or call our anonymous Alert-Line. The Alert-Line is an 800 number you can dial anytime, 24-hours a day, 7 days a week, 365 days per year. We contract with an outside organization for the Alert-Line service, so you can remain anonymous throughout the process. You may also call the Compliance Officer, John Sass at 629-8422.

There are facility specific Privacy Officers; they are your facilities’ Health Information Management Directors. The Corporate Privacy Officer and Compliance Officer is John Sass. The Privacy Officer Hotline is 629-8051.