NORTHEAST
MEDICAL CENTER

HIPAA Privacy Training Manual

This Manual is intended for the training of all personnel who are involved in the treatment of a patient or the payment for that treatment while that patient is at NorthEast Medical Center or any members of its Organized Health Care Arrangement. This Manual is also intended for the training of all personnel who are involved in the healthcare operations of NorthEast Medical Center or any members of its Organized Health Care Arrangement.

Contents

Overview Of Privacy Requirements

This training manual covers the privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of this manual is to acquaint the staff and personnel of NorthEast Medical Center ("NorthEast") and the members of its Organized Health Care Arrangement ("OHCA") as they relate to NorthEast with the confidentiality and patient privacy policies and information security requirements of HIPAA's Privacy Rule ("Privacy Rule") and NorthEast. Examples of personnel who are required to comply with the Privacy Rule are health care providers (physicians, nurses, technicians, etc.), administrative personnel, billing personnel, computer personnel, housekeeping, volunteers, risk management personnel, admissions personnel, and any other person who is employed, works at or volunteers at NorthEast who has or might have access to a patient's private medical information.

The Privacy Rule states that "covered entities" must comply with its regulations. Covered entities include most health care providers, clearinghouses, and health plans. Under the Privacy Rule, personnel involved in the treatment of a patient, in the billing for that treatment or in NorthEast's health care operations must protect the confidentiality of a patient's medical information. NorthEast has many policies and procedures in place to protect the confidentiality and privacy of medical information. This training is about those policies and procedures.

We recognize that patient records are kept in numerous locations, both onsite at NEMC and off-site in clinics. When this manual refers to the "Release of Information Office" or to "Health Information Management", it means that office where the patient's records are being kept and not necessarily NEMC's Release of Information Office or NEMC's Health Information Management.

What Information Is Protected?

Patients are increasingly worried about who has access to their medical information. For example, some fear that their personal health histories could be used to deny them employment or insurance. The Privacy Rule protects the records that hold a patient's medical information and increases the level of confidentiality for those who use and disclose it.

Protected health information is not limited to a patient's clinical and medical information. It includes any information that can identify the patient and is related to their past, present, or future physical or mental health condition, and anything associated with health care services or treatment. For example, it includes billing information, administrative information, or information used for quality assurance or internal reviews. This information is considered "individually identifiable health information" under the Privacy Rule and is afforded the protections of the Privacy Act. This information will be referred to as Protected Health Information ("PHI") in this training manual.

Paper records, electronic records, and oral communications which have PHI are all covered under the Privacy Rule. However, protected health information is also found on IV bags, meal requests, identification bracelets and admission papers. You must carefully examine the information you have to determine if it is protected by the Privacy Rule. ***See NorthEast Policy on Designated Record Sets.***

What Makes Information "Individually Identifiable" Or PHI?

The following list includes those pieces of information, alone or in conjunction with other information, that makes information "individually identifiable" or PHI and, therefore, is subject to Privacy Rule.

- Patient's Name
- Address
- Dates (not including age, unless patient is 89 or older)
- Telephone Numbers
- Fax Numbers
- Electronic Mail Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Beneficiary Numbers
- Account Numbers
- Certificate/License Numbers
- Vehicle Identification and Serial Numbers/License Plate Numbers
- Device Identifiers and Serial Numbers
- Web Universal Resource Locators (URLs) and Internet Addresses
- Biometric Identifiers, Including Finger and Voice Prints
- Full Face Photos
- Any Other Unique Identifying Characteristic

How May You Use PHI?

The Privacy Regulation allows covered entities to use and disclose a patient's PHI as long as they follow the Privacy Rule. However, you must make a reasonable effort to use and disclose only the minimum amount of information necessary to treat the patient, secure payment, and conduct standard organizational duties, such as audits and data collection. In general, this means that you need to evaluate what is the least amount of information you need to do your job. For example, if you are delivering medical supplies to a room for a patient, you do not need to access their entire medical record and history. Likewise, the billing department does not need to know what allergies a patient has – they only need to know what that patient received so they can bill for it. However, a physician does need to know a patient's medical history so they can treat them properly. Likewise, the Corporate Risk Services Department may need to do an audit of all cardiac patient records to do a quality assurance assessment of a certain procedure.

Making minimum necessary determinations is a balancing act. You must weigh the need to protect patients' privacy against the reasonable ability to limit the information that is disclosed, and still deliver quality care, obtain the necessary payment or conduct the health care operation. For treatment purposes, clinical staff and medical providers may use their best judgment to determine the amount of medical information needed for the treatment of a particular patient. This

requirement to use and disclose only that information necessary to accomplish the intended purpose is referred to as the Minimum Necessary standard.

To determine what is necessary to be disclosed and what should be withheld, consider the following questions:

- How much information are you planning to use or disclose?
- How important is it that you use or disclose this information?
- What is the likelihood that further uses or disclosures could occur?
- Where is the information being disclosed (location) and in what form (e-mail, conversation)?

NorthEast's policies and procedures set forth guidelines on what the minimum necessary is based on your category of health care professional. ***See NorthEast Policy for Use and Disclosure of PHI and Minimum Necessary Use and Disclosure*** **and** ***NorthEast Policy on Use and Disclosure of Protected Health Information.***

Patient Notification Of NorthEast's Privacy Practices

NorthEast must provide the patient with a written Notice of Privacy Practices outlining our privacy practices and patients' rights. The Notice must:

- Inform patients of their rights and how to exercise them.
- Disclose NorthEast's privacy practices.
- Inform patients about NorthEast's responsibilities under the law.
- Inform patients about all of the uses and disclosures of protected health information required or allowed by law.
- Explain the process for patients to access their medical records and amend their information.
- Provide the patient with the name and telephone number of NorthEast's Privacy Official who can assist patients with privacy issues.

Patients must receive the Notice at the point that they receive their first service or as soon as possible after emergency care. For most patients, this will be when they check in with Admissions. If you work in the Emergency Department and the patient has not gone through Admissions, you must try to provide them with the Notice as soon as practicable after the emergency is over. The Notice must be visible in high traffic areas and will be posted on the NorthEast web site. In the event NorthEast's privacy practices change, the Notice will be revised to reflect those changes and a new Notice will be given to patients. Patients will sign a written verification that they have been provided the Notice.

You may be asked questions about NorthEast's Notice. Please read the Notice carefully so that you understand your obligations and responsibilities with regard to patient privacy. Also, NorthEast is required to designate a Privacy Official. The Privacy Official is responsible for the development and implementation of privacy policies and procedures and is the point person to receive complaints, inquiries and questions regarding NorthEast's privacy practices and the Notice. Contact the Privacy

Official if you have any questions about the Notice. ***See NorthEast Policy on Designation of a Privacy Official and Contact Person.***

When Is Patient Authorization Required For The Use And Disclosure Of PHI?

In general, you do not need an authorization when:

- you need PHI for treatment, payment and health care operations, as described above; or
- the use or disclosure of PHI is required by law, which will be discussed later.

Based on this, a physician does not need an authorization to use health information to prescribe drugs to a patient. The Admissions department does not need an authorization to enter the patient in NorthEast's system so they can track the patient's admission and discharge (this is a healthcare operation). Finally, the billing department does not need an authorization to file a claim with a patient's insurance. If you are referring a patient to another physician, you also do not need an authorization to release the patient's medical information because this is for the treatment of the patient.

One exception to this rule is that you will need an authorization to disclose psychotherapy notes. Psychotherapy notes are notes recorded by a mental health care provider documenting or analyzing the contents of counseling sessions, group or private. These notes are separated from the rest of the patient's record. The Privacy Rule places a higher degree of protection on this type of information, in part because it can be damaging to a patient if it falls into the wrong hands and the information is of little or no use to those absent from therapy sessions.

When you need to use or disclose a patient's PHI for any reason other than treatment, payment or health care operations, or as required by law, you must have the patient sign an authorization first. For example, the patient must sign an authorization before you can use and disclose health information for a business purpose, such as releasing information to life insurance companies for policy underwriting purposes or providing patient mailing lists to marketing companies. You also need an authorization if a patient wants you to do a physical for an insurance form or for school sports because these are not for treatment.

In general, the Authorization Form must include: the name of the patient, his or her signature, and the person to whom the requested information will be disclosed; a description of the information needed; an expiration date capping the length of time the information can be used; and a warning so that the patient understands that redistributed information may not necessarily continue to be protected. Once a patient has given authorization for you to use or disclose his patient information, he has the right to revoke the authorization at any time and must complete the appropriate form to do so. You can get an Authorization Form from any nursing station, the Release of Information Office, any NorthEast clinic, the NorthEast Intranet and from the Privacy Official.

Specific individuals throughout NorthEast have been trained to work with patients and others requesting the use or disclosure of patient information. It is important that you ensure that an Authorization Form has been received and is in the file when necessary. Any additional questions you have regarding authorization should be directed to the Privacy Official.

Avoiding Authorization Requirements By De-Identifying PHI

Under the Privacy Rule, you may use and disclose health information without a patient's authorization if the information is first "de-identified" or stripped of all of its identifying elements that make it protected health information. De-identification means that the information cannot be used to identify an individual patient. For a complete list of data elements, refer to the section entitled "What Makes Information 'Individually Identifiable' Or 'PHI' " on page 2. Once those elements are removed from the information, you can use and disclose it without having to comply with the Privacy Rule.

You should be aware, however, that it is possible that the remaining elements may identify a patient even if the specific data elements are eliminated. For example, if you perform a study based on a rare diagnosis, even after removal of required data elements, the patient may be identifiable due to the rareness of the illness. Therefore, you should carefully review the information to ensure that it cannot identify the patient in any way. ***See NorthEast Policy on De-Identifying and Re-Identifying Protected Health Information.***

When You Can Disclose PHI Without An Authorization

There are exceptional cases in which covered entities are required to release patient information without an authorization. The following are some of those categories:

- There are laws that require providers to report certain communicable diseases to state health agencies, even if the patient doesn't want the information reported.
- The Food and Drug Administration requires certain information about medical devices that break or malfunction to be reported.
- North Carolina requires you to report suspected child abuse or elderly abuse to the police.
- Police have the right to request certain information about patients to determine whether they should consider the patients suspects in a criminal investigation.
- Certain courts have the rights, in some cases, to order providers to release patient information.
- NorthEast must report cases of suspicious deaths or certain injuries, such as people with gunshot wounds.
- NorthEast must report information about a patient's death to coroners, medical examiners and funeral directors.
- Some public health activities require NorthEast to disclose PHI, such as reporting diseases or collecting vital statistics, required under state and federal law.
- We may be required to disclose PHI to for health oversight reasons, including civil and criminal proceedings, inspections, and audits.
- NorthEast must disclose a patient's PHI to law enforcement officials when they have a warrant, subpoena, or order issued by a judicial officer.

- Disclosure to researchers is permitted, if an institutional review board or privacy board has approved a request for a waiver of the requirement to obtain individual authorization.
- We may also disclose a patient's PHI to organ and tissue procurement organizations, such as when they are in need of a transplant or when they are organ donors and these organizations need to pick up the organs.

If you have questions as to whether you can use or disclose PHI without an authorization, contact the Privacy Official.

Patients Can Opt Out of Certain Disclosures

Patients can object to the use and disclosure of their PHI in certain cases. If they do not object, the information will automatically be included. NorthEast's Notice of Privacy Practices advises patients of this right. However, you may be required to repeat that right to the patients.

The "opt out" option is available for the Facility Directory which lists the patient's name and room number. If someone asks for the patient by name, you can disclose this information if the patient has not opted out of the Facility Directory. If a clergy member asks about the patient, you can also give them the patient's religious affiliation.

While a patient can opt out of being listed in the facility directory (and, therefore, limit who can know the patient is at NEMC), it will not be readily apparent from the records system which patients have exercised their right to opt out. Therefore, you should only discuss a patient's name and room number, general condition or death with a personal representative of the patient or pursuant to the patient's authorization. You should direct all visitors to the NEMC receptionist. The receptionist will be able to determine if the patient has opted out of the facility directory. In an emergency or if the patient is incapacitated, use your professional judgment to determine if it is in the best interests of the patient to disclose their information to a third person.

When To Talk To Family And Personal Representatives

Some patients have personal representatives, such as parents, guardians, spouses or people with health care powers of attorney. This will most likely be an issue when a patient is a minor (a child under 18 who is not emancipated, not married and is not in the military), incapacitated (a patient who cannot make decision for themselves), or has a legal representative.

You may discuss a patient's condition and treatment, or payment for that treatment, with a proper personal representative in the following situations:

- With an **adult patient's** legal personal representative (this includes emancipated minors). This includes people with health care power of attorney, <u>but not</u> people with only a general power of attorney.

- With a **minor patient's** parent, guardian or person standing in the place of a parent (a grandparent, step-parent, teacher, babysitter, etc.). Unless a parent's rights have been terminated or a court order says otherwise, you can discuss the medical condition of a minor

with the non-custodial parent. There are certain situations when you should not disclose a minor's information even to a personal representative. These are:

- If the minor can consent to the treatment without a parent or guardian's permission, such as:
  (a) Diagnosis and treatment of sexually transmitted diseases;
  (b) Pregnancy and family planning services;
  (c) Alcohol/drug abuse treatment; and
  (d) Emotional disturbance.
- If the court has named someone else the personal representative.
- If the parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between NorthEast and the minor.
- If you believe the personal representative is abusing, neglecting or endangering the patient.

- If the patient is **dead,** then you can discuss their information with the patient's executor, administrator or person with legal authority to act on behalf of the estate. This includes family members with a durable power of attorney.

You must verify and document a person's authority to be the patient's personal representative. This includes documenting the name and contact information of the personal representative, how they qualify as a personal representative (keep copies of any proof such as health care powers of attorneys), and a description of what and why you disclosed to them, including any reasons why you were prevented from disclosing to them. ***See NorthEast Policy on Personal Representatives.***

Fundraising

The Privacy Rule allows NorthEast to use a patient's demographic information and dates of service for certain fundraising efforts without a patient's authorization. Demographic information includes names, addresses and other contact information, age, gender, and insurance status. It does not include information about illness or treatment.

Permitted fundraising activities include requests for contributions and event sponsorships. They do not include royalties or remittances for the sale of products to third parties. Patients must be given the option of opting out of future fundraising. This will be addressed in the fundraising materials sent to the patient.

Only hospital-based foundations and certain business associates can receive fundraising information. All marketing and fundraising activities must be approved and carried out by the NorthEast Medical Center Foundation Office. ***See NorthEast Policy on Fundraising.***

Marketing

Usually, marketing requires an authorization from the patient. However, you are allowed to have face-to-face discussions with the patient or give them a promotional gift of nominal value. For example, you can still give a patient free samples without needing an authorization.

You can also discuss certain products and benefits with the patient without it being marketing and without needing an authorization:

- You can describe a health-related product or service provided by NorthEast.
- You can discuss participating providers in the NorthEast network, or health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits. You can also discuss products and services for the patient's treatment.
- You can discuss case management or care for the patient.

Any other communications which encourage a patient to buy a certain product or service, or any disclosures of patient information to another provider in exchange for money, requires an authorization and must be approved in advance by Strategic Planning and Market Development . ***See NorthEast Policy on Marketing.***

Media Inquiries

If the media asks about a patient, they should be referred to NorthEast's Strategic Planning and Market Development Department. Please call the NorthEast Media Representative on call at (704) 783-3000. For example, if a racecar driver is injured and brought to NorthEast for treatment, you should not give any information to the media and refer them to the Media Representative. Even then, the Media Representative should only confirm the driver's admission and general condition. No information regarding individual patients will be released without the authorization of the patient or the patient's authorized representative. ***See NorthEast Policy on Media and Patient Information.***

Patient Right To Access and Receive Their PHI

Patients can request access to their PHI kept in medical records, billing records, management records or any other records that NorthEast uses to make patient decisions. To request access, the patient must check the "Myself" box on the Authorization Form. These forms are available at any nursing station, the Release of Information Office, any NorthEast clinic, the NorthEast Intranet and from the Privacy Official. All completed forms should be sent to Release of Information Office.

In general, a patient will be allowed to access his requested records. The Release of Information Office will be responsible for giving notice to the patient of the access and coordinating the patient's access to those records within certain time limits.

In certain situations, however, a patient is not entitled to access their medical records. These include:

- Psychotherapy notes (notes recorded, in any medium, by a mental health professional documenting or analyzing the contents of conversation during a private counseling

session or in a group, joint, or family counseling session and that are separated from the rest of the individual's medical record).

- Information gathered for a legal proceeding (civil, criminal or administrative).
- Information subject to the Clinical Laboratory Improvement Amendments of 1988 ("CLIA"), which only allows clinical personnel ordering laboratory tests to access the test results or reports and does not allow patients to access this information.
- The patient is an inmate of a correctional facility or NEMC is acting under the direction of a correctional facility and the release of PHI could jeopardize the health, safety, security, custody, or rehabilitation of the patient or other inmates, or the safety of any officer, employee, or other person at the facility responsible for transporting the inmate.
- The patient is participating in research which includes treatment and he has agreed not to access the PHI while the research is in progress. However, the patient may be given access to the PHI when the research is completed.
- The patient's request would require access to PHI that is contained in records that are restricted by the Privacy Act.
- Someone other than a health care provider gave NEMC the patient's PHI under a promise of confidentiality, and allowing the patient to access the PHI would likely reveal the source of the information.

The denial of the access request in these situations will be automatic and the patient does not have a right to have that denial reviewed. The Release of Information Office will be responsible for notifying the patient of the denial in writing within certain time frames.

Sometimes, a health care provider may feel that the patient should not be allowed to access his medical record. This would occur if:

- The health care provider determines that a patient's access to the record is likely to endanger the life or physical safety of the patient or another individual.
- The PHI references another person who is not a health care provider and the health care provider determines that allowing the patient to access this information will likely cause substantial harm to that person.
- The health care provider determines that allowing a patient's personal representative access to the file could result in harm to the patient or another individual.

The health care provider should flag the file so that the Release of Information Office will know that the access request should be denied but that the patient must be advised they have a right of review. If the patient invokes that right of review, the Release of Information Office will forward the file to the Privacy Official

If there is a review, a licensed health care provider will be assigned to review the request and make a reasonable decision about whether to grant or deny the request within a certain time of it being submitted by the patient. If the request is granted, the Release of Information Office will give the patient written notice of the decision and either provide actual access to the patient or, if they agree, provide them with a summary. If the request is denied after review, the patient may request that the

denial be reviewed by a different person in certain situations and subject to the processes set forth in NorthEast's policies and procedures.

NorthEast may charge reasonable fees for copying and mailing the PHI to the patient. A copy of the request, all decisions and all notifications should be kept in the patient's file, in addition to other documentation. ***See NorthEast Policy on Patient Right to Access and Receive Protected Health Information.***

Patient Right To Request An Amendment To Their PHI

Patients have the right to request that NorthEast amend their PHI. A patient must complete the Request for Amendment of Protected Health Information Form. These are available at any nursing stations, the Release of Information Office, any NorthEast clinic, the NorthEast Intranet, and from the Privacy Official. All forms should be sent to Health Information Management.

If you have first hand knowledge about the information the patient wants to amend, you will work with the Privacy Official to review the information and make several determinations about its accuracy and content. Based on that review, the information may or may not be amended. If the request is denied, the patient has a right of appeal and the Privacy Official may contact you again.

A request for amendment will be denied if:

- The PHI or record was created by someone other than NorthEast,
- The PHI the patient requested to amend was not part of the designated record set covered by the Privacy Rule,
- The PHI or record the patient requested to amend was psychotherapy notes, it was information compiled in anticipation of or for use in a civil, criminal or administrative proceeding, or subject to CLIA restrictions, or that the PHI or
- Record was accurate or complete.

If the request is denied, a patient has the right to file a disagreement statement with the Privacy Official. A decision to grant or deny a request for amendment must be given in 60 days, but can be extended an additional 30 days if necessary and if proper notice is given to the patient.

The Privacy Official and Health Information Management will be responsible for amending the patient's health information. A health care professional should not amend the record. The information that is amended will not be deleted; instead, the record will include both the original information and the amended information. The record will also include any disagreement statements filed by the patient and the rulings on those statements. NorthEast must notify the people who have the information in their own file so it can be properly amended, as well as those people identified by the patient as needing the amended information. ***See NorthEast Policy on Amendment of Protected Health Information.***

Patient Right To An Accounting Of The Disclosures Of Their PHI

A patient has the right to request an accounting of when, what, to whom and why their PHI was disclosed. NorthEast has computer programs in place to account for these disclosures electronically.

The patient must complete the Accounting of Disclosures of PHI Form. These are available at any nursing stations, the Release of Information Office, any NorthEast clinic, the NorthEast Intranet, and from the Privacy Official. All forms should be forwarded to Health Information Management.

A patient can request an accounting of most disclosures of their PHI, except the following:

- Disclosures for health care treatment, payment, or operations;
- Disclosures to the patient;
- Disclosures incident to permitted disclosures;
- Disclosures pursuant to a valid authorization;
- Disclosures for the facility's directory or used to notify other's involved in the patient's care;
- Disclosures to national security or intelligence;
- Disclosures to correctional facilities or law enforcement officials;
- Disclosures for a limited data set; or
- Disclosures made prior to April 14, 2003.

Even though not all information is provided to the patient, NorthEast's system will keep track of every personnel's access of a patient's information. Therefore, you should not access records of patients who are not under your care. For example, you should not be checking the medical status of the racecar driver if you are not on his treating team. If you violate the policy, NorthEast will take disciplinary action.

If an accounting of disclosures is provided, the accounting will include the date of the disclosure; the name of who received the PHI and their address if known; and a brief statement that advises the patient why the disclosure was made or a copy of a written request for the information.

The Privacy Official or his/her designee will be responsible for giving the patient the accounting of disclosures. You should cooperate with any requests or inquiries from the Privacy Official related to the accounting. ***See NorthEast Policy on Accounting of Disclosures of Protected Health Information.***

What You Should Know About Business Associates

Sometimes, NorthEast uses outside people and companies to help us with our operations who need to access PHI to do their jobs. These people and companies are known under the Privacy Rule as "Business Associates". Some examples of NorthEast's Business Associates are lawyers, accountants, healthcare consultants, transcription agencies, and software vendors. The list of possible Business Associates for NorthEast is extensive, so this is a key area of concern for Privacy Compliance.

NorthEast cannot disclose PHI to Business Associates unless the two parties have a contract. The type of contract used is called a Business Associate Agreement. The Business Associate Agreement

must contain specific provisions, including a confidentiality clause that holds Business Associates accountable for protecting private patient information. The Business Associate cannot use or further disclose the information in a manner that violates the Privacy Rule. In fact, they must safeguard the information as if they were the covered entity.

NorthEast must ensure that a Business Associate's subcontractors also follow the Privacy Rule and that the Business Associate is required to report any breach of privacy to NorthEast. NorthEast must take the necessary steps to decrease the potential for misuse and disclosure of PHI by Business Associates and may terminate a Business Associate if they fail to meet their duties of privacy and confidentiality. If termination of the contract is not possible, then NorthEast must report the Business Associate to the Secretary of the Department of Health and Human Services.

Information provided to a Business Associate should be the minimum amount necessary to accomplish the intended purpose. Health care providers can rely upon their professional judgment of the Business Associate to determine the information needed. NorthEast's Legal Department is coordinating Business Associate Agreements and has a standard Business Associate Agreement that is located on the NorthEast Intranet. Any Business Associate Agreements presented to you by a Business Associate should be submitted to the Legal Department and can only be signed by an authorized NorthEast Vice President. ***See NorthEast Policy on Business Associates.***

Computers And Privacy

We use computers in almost every aspect of operating NorthEast, treating our patients and billing for our services. Therefore, NorthEast has put certain safeguards in place to protect the privacy of the PHI which is on our system and to restrict who can access that PHI. You will be assigned a password that is only intended for your use. DO NOT share the password with any other person, or this will be considered a violation of NorthEast policy and result in disciplinary action. Make sure that when you are done using the computers, you log off. Leaving a computer screen on with a patient's PHI for anyone to see is considered a violation of the Privacy Rule.

Computers are only returned, discarded or donated through the Information Systems Department, which will remove PHI and software from the computers. Only Information Systems employees will load software. Information Systems will work with software vendors regarding maintenance or installation services and make sure that they have signed a Business Associate Agreement before they can perform such services. Contact the Information Systems Department with any issues about computers and software.

Practical Steps For Protecting PHI

Protecting PHI is a top priority while performing your job. Computers, cell phones, and hand held devices are technological necessities, but using them carries extra responsibility in the privacy era. Taking a few precautions can go a long way to avoiding a HIPAA violation:

- Avoid discussing patient information in public areas such as elevators, cafeteria, and the gift shop.
- Do not leave patient information unattended where others can see it. This is especially important in public buildings, provider locations, and areas with heavy pedestrian traffic.

- When you are checking someone into the hospital, do not discuss their medical information so other patients or guests can hear it.
- When you are done using paper patient information, return it to its appropriate location (i.e., Health Information Management or a file at a nursing station.)
- When you are done accessing electronic patient information, log off the system. Do not leave the information visible on an unattended computer monitor. Do not share passwords. Sharing your password is grounds for sanctions.
- **DO NOT** place PHI in the trash can. Make sure all paper patient information is shredded before being disposed.
- When faxing patient information, make sure you are faxing to a dedicated fax machine in a secure location and that you put a cover sheet on the fax. Call the person you are faxing and verify you have the proper fax number before sending the fax. Do not leave faxes lying around unattended.

See NorthEast Policies on Faxing and Privacy Safeguard..

Cooperating With DHHS

The Department of Health and Human Services is the federal agency that is responsible for ensuring that covered entities are complying with the Privacy Rule. Therefore, DHHS may investigate our records and practices. The Privacy Official will be responsible for handling all communications and documents with DHHS. If you have any questions or are contacted by DHHS, call the Privacy Official. ***See NorthEast Policy on Compliance with the Department of Health and Human Services***

What Happens If You Don't Comply With The Privacy Rule

It is very important that you follow NorthEast's policies and procedures or the Privacy Rule. Violating the Privacy Rule and NorthEast policies and procedures is very serious. If you violate them, you will be reprimanded. Reprimands will range from a Final Written Reprimand to Termination. ***See Personnel Policies HR 5.06 and HR 5.08***

You will not be sanctioned if you are disclosing PHI to report it in good faith to a health oversight agency, to report to an authorized public health authority, to report NorthEast for violations or dangerous, unethical or illegal conduct, or to file a complaint with the Department of Health and Human Services. ***See NorthEast Policy on Retaliation for Complaints.***

The federal government may also impose certain sanctions under HIPAA. For civil penalties, $100 per person, per violation with a maximum of $25,000 per person, per standard, per year. For criminal penalties, 1-10 years in jail and up to $250,000 in penalties. ***See NorthEast Policy on Sanctions and Mitigation for Privacy Violations.***

