

PROTECTING PATIENT PRIVACY

What is Protected Health Information (PHI)?

PHI can be in any form, such as:

* Patient medical record	* Telephone calls and voice mail about patients
* Fax transmissions that contain patient information	* Patient information in our computer systems
* Conversations between clinical staff about treating patients	* Email, text message, or Instant Messages (IMs) that contain patient information

And can be found on:

* X-rays	* Prescriptions
* Photographs	* Lab work
* Test results	* Billing records
* Claim data	* Explanation of Benefits
* Referral Authorizations	* Research Records

PHI that is contained on computer systems is known as **ePHI** (electronically protected health information)




Note: Even the fact that an individual is a patient of ours, or pays us for services, is Protected Health Information.

Protecting PHI

We need to be *very careful* with patient health information. Patients expect us to protect their information from anyone who does not need to know it. Protecting patient information is the responsibility of each one of us!

Note: If you have a concern about patient privacy, or if something doesn't seem right, ASK!!!

Remember:

-  **Don't snoop or gossip**
-  **Keep your voice down**
-  **Respect patient health Information – DISPOSE OF IT PROPERLY!!!!**
-  **Always lock workstation when unattended**

PHI Identifiers

Any identifier on the following list about the patient or the patient's relatives, employers or household members is considered Protected Health Information:



Note: You can "de-identify" health information by removing **all** of the identifiers listed below. "Deidentified" information is not subject to the HIPAA Privacy Rule and can be freely disclosed.

* Names (First, Middle, Last)	* Geographic subdivisions
* All elements of dates directly related to patient (i.e., birth, death, admission and discharge)	* Telephone Numbers
* Fax numbers	* E-mail addresses
* Social Security Numbers	* Medical record numbers
* Health plan numbers	* Account numbers
* Certificate/license numbers	* Vehicle identifiers
* Device identifiers and serial numbers	* Website address (e.g., a Universal Resource Locator (URL) or Internet Protocol (IP) address numbers
* Biometric identifiers such as finger prints	* Full face photographic images
* Any other unique identifying number, characteristic, or code	* Age greater than 89 (due to the 90 year old and over population is relatively small)

USING AND DISCLOSING PHI

Verification and Minimum Necessary

The two key rules of being careful about releasing patient information are:

-  **Verify the Requester:** Before you disclose patient information, confirm that the requestor is entitled to receive it. There are many ways to verify that a person is who they say they are. For example, you can identify a patient by name and address, Social Security Number, or date of birth. A doctor's office can be identified by name and tax ID number. A police officer or government official can be identified by a valid badge.
-  **Provide Minimum Necessary Information:** Minimum Necessary Information means: tell the requestor ONLY what he or she needs to know. Do not offer additional information.

Note: *Minimum Necessary* does not apply to disclosing patient information to providers for treatment purposes.

VERIFY THE REQUESTER	MINIMUM NECESSARY
✓ Perhaps we already know the requester	✓ Once you're comfortable with the requester and the request, give out only what the person really needs to know
✓ Perhaps we have made a very simple check like a birth date, date of service, Social Security Number, or photo I.D.	✓ Our co-workers usually only ask for what they need
✓ Perhaps we have asked for the requestor's business telephone number and made a callback	✓ Unusual requests from individuals you don't know are risky. Limit the information you give out – no more than exactly what they are authorized to receive

Patient Authorization for Release of PHI

If we want to release a patient's health information for purposes other than treatment, payment, and routine health care operations, then generally we must ask the patient to sign an authorization.

Q. What should I do if a physician calls and wants information about a patient?

A. A patient authorization is **not** needed to release PHI for treatment purposes. Verify that the physician is who he says he is, and that he is involved in the patient's treatment. Then you can disclose the information that the physician is requesting.

Note: If you know the physician, you don't need to verify.

Remember: *Minimum Necessary* does not apply to disclosures made to physicians for treatment purposes.

An authorization is specific to the particular situation for which it is being requested, and it lasts for only a limited period of time.

Some examples where authorization is required before we release a patient's information are:

- ✚ A patient signs an authorization form to release PHI to an insurance company to obtain disability coverage.
- ✚ A pregnant patient signs an authorization to have her pregnancy status released to a business that markets infant care products.
- ✚ A researcher requests authorization from a patient to participate in a clinical trial.

Disclosure to Family and Friends

Certain disclosures are permitted, provided that we have given the patient an opportunity to object to the disclosure. These include disclosures to family and friends.

- ✚ We must ask the patient if he or she objects to disclosing health information to family or friends.
- ✚ If the patient objects, then we are not permitted to discuss the patient's health condition with family or friends.

Note: If the patient is not able to tell us if he objects, such as in an emergency situation or when a patient is unconscious, then we must use our best professional judgment to decide whether to talk to a family member or friend.

Q. A friend is worried because his girlfriend is in the hospital. He asked me to find out anything I can. Should I try to find information for my friend?

A. No. You should not even tell him that his girlfriend is in the hospital. Tell your friend to call or visit the information desk. If the patient has agreed to have her information available, the information desk staff can give it to him.

Incidental Disclosure of PHI

Incidental Disclosure of PHI is defined as a secondary disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use or disclosure of PHI.

Examples of incidental disclosures that are permitted:

PERMITTED DISCLOSURE NECESSARY CONDITIONS

◆ Use of sign-in sheets	◆ Provided that the sign-in sheet does not contain information on the reason for the patient's visit
◆ The possibility of a Confidential conversation being overheard	◆ Provided that the surroundings are appropriate for a confidential conversation and voices are kept down
◆ Placing patient charts outside exam rooms	◆ Provided that unauthorized public traffic is not permitted in the area of the exam rooms and face sheets are turned towards the wall
◆ Use of white boards	◆ Provided that only the minimum information needed for the purpose of the white board is used
◆ X-ray light boards that can be seen by passers-by	◆ Provided that patient x-rays are not left unattended on the light board

◆ Calling out names in the waiting room	◆ Provided that the reason for the patient's visit is not mentioned
◆ Leaving appointment reminder voicemail messages	◆ Provided that the minimum amount of information is disclosed

EMPLOYEE AS A PATIENT

As an employee, you are encouraged to seek world class care here at Einstein! Here are a few key items for you to remember.

- ✚ Your status as an employee does not afford you special care or privileges not extended to the patient population served by the hospital.
- ✚ When you schedule an appointment you are doing so as a patient. The time, location, date, and nature of your appointment is privileged information between you and the department where you are seeking care.
- ✚ When you arrive for your appointment you will be acting in the capacity of a patient – and you can expect to be treated by the staff as a patient.
- ✚ It is possible that you may be recognized as an employee by a staff member or another patient at the facility at the time of or enroute to your appointment. Being recognized as an employee does not permit your status as a patient – or the nature of your care - to be divulged to others unless they are directly involved in your care or you expressly give permission to discuss your status to those not involved in your care.
- ✚ Information that is related to your care (such as physician and nursing notes or laboratory results entered in your Medical Record) will remain private. The release of your information for certain situations (such as billing or collaboration between physicians involved in your care) is governed by Federal law (e.g., HIPAA for example.)

Q. A friend is worried because he saw his girlfriend coming out of the OBGYN Clinic at the hospital. He knows that I work in OBGYN and that I have access to her Medical record. He asks me to look at her Medical Record and find out anything I can. Should I try to find information for him?

A. No. You may have been involved in her care and also had access to her medical record; however, the nature of the care given her cannot be divulged by you. Doing so would be a breach of her privacy rights under Federal Law.

Q. I work in an outpatient clinic here at Einstein. I am also a patient at the same facility. What assurance do I have that my co-workers will keep my condition as well as my medical information private when I am being seen and treated as a patient?

A. Being recognized as an employee does not permit your status as a patient – or the nature of your care - to be divulged to others unless they are directly involved in your care. If a coworker deliberately accesses your medical record without being authorized to do so this will be considered a breach of your privacy rights under current Federal Law.

SANCTIONS FOR IMPROPER DISCLOSURE

On February 17, 2009, President Obama signed into law the HITECH Act as part of the American Reinvestment & Recovery Act (ARRA) of 2009 (Public Law 111-5.) The HITECH Act contains provisions that dramatically extend HIPAA's reach. It is important to understand that the ARRA (HITECH Act) is a law and not a regulatory document. The effective date of HITECH was February 17, 2010.

Some of the substantial changes to HIPAA under the HITECH Act include:

Heightened Enforcement and Increased Penalties – Failure to comply with HIPAA due to willful neglect will result in mandatory penalties. The penalties assessed are based on whether the violation was made without knowledge, due to reasonable cause, or due to willful neglect. Education will be a major factor in maintaining compliance with current law (i.e., HIPAA) along with the addition of new mandates found within ARRA and the HITECH Act.

Categories of Privacy Incidents

- ✚ Unintentional breach of privacy or security that may be caused by carelessness, lack of knowledge, or lack of judgment, such as a registration error that causes a patient billing statement to be mailed to the wrong guarantor.
- ✚ Deliberate unauthorized access to PHI without PHI disclosure. Examples: snoopers accessing confidential information of a VIP, coworker, or neighbor without legitimate business reason; failure to follow policy without legitimate reason, such as password sharing.
- ✚ Deliberate unauthorized disclosure of PHI or deliberate tampering with data without malice or personal gain. Examples: snooper access and redisclosure to the news media; unauthorized modification of an electronic document to expedite a process.
- ✚ Deliberate unauthorized disclosure of PHI for malice or personal gain. Examples: selling information to the tabloids or stealing individually identifiable health information to open credit card accounts.

Hospital policy provides for sanctioning in the event PHI is improperly disclosed.

- ✚ Guidance is located in HR 121 – Sanctions Policy
- ✚ Employees that fail to comply will be disciplined
- ✚ Sanctions range from a warning up to dismissal

PATIENT PRIVACY RIGHTS

The new HIPAA Privacy Law gives new civil rights, known as Patient Privacy Rights, to all our patients. These rights give patients more control over how their health information is shared and communicated.

Right to Obtain a Copy of Our Notice of Privacy Practices

Patients have the right to receive a copy of the hospitals *Notice of Privacy Practices*.

Right to File a Complaint

If a patient believes that their confidentiality has been breached or we have violated the law, he or she has the right to file a complaint with us, or directly with the Secretary of the Department of Health and Human Services.

Right to Request Restrictions On Certain Uses and Disclosures

Patients have the right to request restrictions on certain uses and disclosures of their health information.

- ✚ Patients can ask us to limit how we use and disclose their health information.
- ✚ The law does not require us to accept or agree to a patient's request to restrict the use or disclosure of their health information.

- ✚ If we agree to accept the patient's restriction, we must adhere to the agreement. If we do not agree to the restriction, we must inform the patient that we do not accept the restriction.

Right to Select How to Receive Health Information

Patients have a right to choose how they receive their health information.

- ✚ Patients can request that we communicate with them in a certain way, such as by mail or fax, or at a certain location, such as home address or post office box.
- ✚ We are required to do our best to accommodate reasonable patient requests for confidential communications.

Right to See and Copy Records

Patients have a right to read and obtain copies of their medical record.

- ✚ Patients can look at and receive a copy of certain medical and billing records.
- ✚ We can deny the request if the information is in mental health records, the information was gathered for a court of law, or releasing the information might harm the patient or another person.

Right to Update Records

Patients have the right to update their medical records.

- ✚ If patients believe that a piece of important information is missing from their medical record, they can request that we add an amendment to their medical records.
- ✚ We may deny the patient's request to amend their medical record if the information being amended was not created by us, if we believe the information is already accurate and complete, or if the information is not contained in records that they would be permitted to see and copy.

Right to Obtain a List of Disclosures

Patients have a right to get a report of the disclosures we have made of their health information.

- ✚ We are not required to give the patient an accounting of the disclosures that we have made for purposes of treatment, payment, or health care operations.
- ✚ We are not required to include disclosures for which we received written patient authorization or certain other disclosures excluded by law.
- ✚ The report must contain specific information, including the dates, names, and information disclosed.

SECURITY OF INFORMATION IN COMPUTER SYSTEMS

The HIPAA Privacy Rule calls for us to take "appropriate safeguards" to protect the privacy of patient information. This includes the patient information in our computer systems. We need to take special precautions that this information is:

- ✚ Not accessible to people not authorized to see it
- ✚ Not damaged or changed maliciously or by mistake
- ✚ Readily accessible to providers who need it quickly
- ✚ Never to access data you are not authorized to use

◆ Logging off	◆ Log off your computer before leaving it, and do not use anyone else's computer unless you are authorized to do so
◆ Passwords	◆ Never share your password or leave it out where others can see it
◆ Computer screen	◆ Never leave patient information on your computer screen where it can be viewed by others who do not need to know
◆ Records	◆ Never create, change, or delete records unless you have specific authority to do so
◆ E-mail, Text messages and/or Instant Messages (IMs)	◆ Never use e-mail to send PHI unless it has been encrypted to protect it from unauthorized access. Do not send PHI via a text message or IM.
◆ Taking a picture of a patient with a cellular Phone, camera, or other similar device.	◆ Taking a picture of a patient is prohibited under most circumstances and may require the express written permission of the patient.
◆ Expectation of Privacy	◆ None. EHN considers all correspondence, regardless of form, as being corporate owned and therefore subject to review.

Notes:

Contact Information

- Chief Compliance Officer: (215) 456-7084
- Health Information Management (HIM): (215) 456-6800
- Information Security & Privacy: (215) 456-8022
- Information Systems HELP Desk: (215) 456-8033
- Legal Department: (215) 456-7373
- Risk Department: (215) 456-6397

To make an anonymous report of any suspected violation of a policy, procedure, rule, regulation or law contact the

Compliance Hotline

1 – 866 – 458-4864