

## ***Health Information Portability and Accountability Act (HIPAA)***

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, includes the Standards for the Protection of Individually Identifiable Health Information – better known as the Privacy Rule. Most Health care providers must comply with the new requirements by April 14, 2003. The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records as well as other personal health information.

- ❖ It gives patients additional rights for more control over their information.
- ❖ It sets boundaries on the sharing of this information
- ❖ It establishes appropriate safeguards that health care providers and others must achieve in order to protect this information
- ❖ It holds violators accountable, with civil and criminal penalties that can be imposed if privacy rights are violated

The purpose of the following information is to provide you with a *general* overview of the HIPAA Privacy Rule. Additional policies and procedures related to the Rule will provide further job-specific guidance. This job-specific training will be the responsibility of departmental leaders as these policies and procedures become available.

### ***Definition of Terms***

**Protected health information, or PHI**, is any information that individually identifies a person as it relates to health such as:

- Name
- Address
- Employer
- Relative's name
- Date of birth
- Telephone and fax #
- Email address
- Social security #
- Medical record number
- Member or account numbers
- Certificate #
- Voiceprint
- Fingerprint
- Full facial photograph
- Codes
- Driver's license number

And any other identifying characteristic, such as occupation, which may identify someone.

**Treatment** generally means providing, coordinating, & managing healthcare and related services. It includes referral to and consultation with other healthcare providers about healthcare and related services.

**Payment** generally means the activities undertaken by a healthcare provider to obtain or provide reimbursement for providing healthcare. This includes pre-authorization/pre-certification, utilization review, collection activities, billing, and other related activities.

**Operations** generally means activities such as QA, case management, training programs for students, auditing, legal review, business management, planning and development and other such activities related to our business as a healthcare provider.

Treatment, Payment and Operations may be referred to later during this session as T/P/O.

**Use** generally means sharing of PHI amongst 'staff, students, or faculty'.

**Disclosure** generally means the sharing in any manner of PHI with other parties.

Generally, information can be disclosed to health care agencies for the purposes of T/P/O.

#### *PERMITTED USES AND DISCLOSURES*

***GENERALLY, YOU ARE PERMITTED TO USE AND DISCLOSE PHI FOR THE PURPOSE OF TREATMENT, PAYMENT AND OPERATIONS (T/P/O).***

#### ***OTHER PERMITTED USES AND DISCLOSURES GENERALLY INCLUDE:***

- ***TO BUSINESS ASSOCIATES WHO ARE PROVIDING A SERVICE ON OUR BEHALF***
- ***AS DIRECTED BY A PATIENT ON A VALID AUTHORIZATION FORM***
- Those required by law (i.e. State reporting of births and deaths into databases)
- For judicial and administrative proceedings (i.e. in response to a subpoena)
- For organ and tissue donation
- For the purpose of Research
- To avert serious threat to public safety

Refer to agency policies on permitted uses and disclosures for the complete list.

#### **THE AUTHORIZATION REQUIREMENT**

For some of the permitted uses and disclosures, a written patient authorization is required. The Privacy Rule mandates that standard statements and elements be included in these forms.

Refer to your assigned agency policy on Authorization for Release of Information forms for information about authorization requirements. Contact Health Information Management or the records custodian for the particular entity in which the records are maintained for assistance with regard to authorization forms.

#### **THE MINIMUM NECESSARY RULE**

Healthcare providers must make a reasonable effort to use and disclose only the minimum amount of PHI necessary to do their jobs. However, providers can disclose PHI requested by other healthcare providers if the information is necessary for treatment of a patient.

Healthcare agencies receiving federal funding are mandated by the Privacy Rule to define the minimum amount of PHI necessary by job class to perform job functions. Refer to your job description or contact your Manager for your specific PHI privileges.

#### **RIGHT TO NOTICE OF PRIVACY PRACTICES**

Patients have a right to adequate notice of all the ways we may use or disclose their PHI as well as our legal duties in protecting their information. We must make the notice available as follows:

- ❖ On the first treatment date even if the service provided is electronic
- ❖ As soon as is practical in an emergency treatment situation
- ❖ To those who ask for it

- ❖ On your assigned agency web site
- ❖ Posted in a prominent location at all physical service delivery sites

Healthcare agencies must make a good faith effort to obtain a written acknowledgement of receipt of the notice or document our good faith effort to attempt to obtain it except in emergency situations. These documents must be retained for a period of 6 years.

### **RIGHT TO REQUEST A RESTRICTION**

Patients have a right to *request* a restriction on how we use and/or disclose their PHI:

- to carry out treatment;
- for payment;
- for our operations
- to others involved in their care; and/or
- when there is a request to notify family about patient information

According to our policy, requests must be made in writing. We are not required to agree to a restriction, but the entire organization must abide if we do agree to a restriction.

For example, a hospital patient is diagnosed with high blood pressure. He requests that his wife not be told about the diagnosis. It may seem easy enough to abide by this request to restrict. But following the policy is essential. There may be other departments that will see this diagnosis and disclose the information as part of their job functions unaware that you have agreed to a restriction. (i.e. the wife might see the diagnosis in the mailed billing statement).

Therefore, if a patient requests a restriction of uses or disclosures of their PHI, refer to the appropriate agency policy. Requests for restrictions are handled by Health Information Management or the records custodian for the particular entity in which the records are maintained.

### **RIGHT TO ACCESS**

Patients have a right to inspect and obtain a copy of most PHI about them. A request by a patient to view or receive a copy of PHI must be made in writing. These requests should be forwarded to Health Information Management or the records custodian for the particular entity in which the records are maintained.

### **RIGHT TO REQUEST AN AMENDMENT**

Patients have a right to request an amendment to PHI. We are not required to agree to a request for an amendment to records.

According to most agencies' policy, these requests must be made in writing. Therefore, requests by a patient to amend their PHI should be forwarded to Health Information Management or the records custodian for the particular entity in which the records are maintained.

### **RIGHT TO AN ACCOUNTING**

Patients have a right to request a report of certain disclosures that we make to outside parties. This does not include permitted disclosures for T/P/O, when a HIPAA compliant authorization to release information has been signed, or for disclosures made to the patient. Some examples of the disclosures we will need to include in such a report are:

Disclosures **required by law** such as mandatory State reporting of:

1. Deaths
2. Births

3. Suspected child or elder abuse
- Disclosures **for Public Health purposes** such as:
1. Adverse drug events
  2. Tracking of medical devices
  3. Notification of a school of exposure to an infectious disease

Disclosure for some **Research activities**

To determine which disclosures you make that need to be tracked, and how to track them, refer to your assigned clinical agency's policies on Accounting for Disclosures.

According to some agency policies, these requests by the patient must be made in writing. If a patient requests a report of the disclosures made regarding their PHI, they should be referred to the appropriate department in the clinical agency.

### **RIGHT TO REQUEST CONFIDENTIAL COMMUNICATION**

Patients have a right to request to receive communication of their PHI from us by alternative means or at alternative locations. We must accommodate reasonable requests. For example a patient may ask that the results of a lab test be called to their work phone number and not their home phone number. If a patient requests this from you, refer to our policy. For questions, contact the Privacy Official at your assigned clinical agency.

### **REASONABLE SAFEGUARDS**

We must protect patient information from inappropriate disclosure. Some examples of policies related to reasonable safeguards that we have in place already include:

- ❖ Using locked recycle bins & shredders
- ❖ Keeping charts and records out of public view
- ❖ Logging off your computer and not sharing passwords
- ❖ Locking file cabinets with PHI
- ❖ Covering PHI when mailing
- ❖ Restricting conversations about patients to private areas

It is your duty to ensure that you follow these and any other current or new policies that will safeguard PHI routinely.

### **VERIFICATION OF IDENTITY**

Before PHI can be disclosed, we have a duty to verify the identity of the person requesting the information. Refer to our policy for suggested methods to verify identity before disclosing PHI.

Some examples include:

- Asking for identification such as a driver's license
- Asking for information that the patient would know such as mother's maiden name, patient's middle name, or patient's place of birth

Refer to your assigned clinical agency's policy on Verification of Identity for further guidance.

### **PATIENT COMPLAINT PROCESS**

If a patient has a complaint or concern with regard to their privacy rights, they can be referred to the health care agencies Patient Relations Department or to the Office for Civil Rights. The complaint process for patients related to privacy rights is, also, included in the Notice of Privacy Practices booklet.

**PENALTIES**

Failure to comply with the Privacy Rule could result in civil and/or Federal criminal penalties including monetary fines up to \$250,000 and up to 10 years in prison. The Federal government is serious about protecting a patient's right to privacy of their information.

Therefore, most clinical agencies may impose disciplinary action for non-compliance related misconduct regarding HIPAA.