Overview of HIPAA Privacy Standards

HIPAA stands for Health Insurance Portability & Accountability Act. One purpose of HIPAA, the Privacy Rule is to improve the efficiency of the healthcare system and to provide standards for security and privacy of a patient's health information.

The HIPAA Privacy Rule creates national standards for the protections of an individual's health information. The rule provides for the following:

- More control of an individual's health information by the individual;
- Boundaries for the uses and disclosure of protected health information;
- The implementation of physical safeguards to help ensure that health information remains confidential; and
- Violators are held accountable, with civil and criminal penalties.

The HIPAA Privacy Rule applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

HIPAA protects "individually identifiable" health information. This information can be transmitted or maintained in any form or medium, which includes information transmitted orally, stored or transmitted on paper and/or electronically.

Health information is considered identifiable & protected health information (PHI) if any of the following is present:

- Patient's Name;
- Address or zip code;
- Month and date of service or other relevant date;
- Date of Birth;
- Telephone and/or fax number;
- E-mail address;
- Social Security Number;
- Medical Record or patient account numbers;
- Health plan beneficiary number;
- Device identifiers or serial numbers;
- Biometric identifiers, including finger & voice prints;
- Full face photographic images or other images;
- Web Locators (URLs) or Internet Protocol (IP) addresses;
- Any other unique identifying number, characteristic, or code.

This information can be found in paper charts, computerized patient records, clinical research records and billing records.

There are penalties for violations of the HIPAA Privacy Rule. The maximum penalties can range from $100 to $50,000 per violation. Violations may include imprisonment up to 10 years.

A HIPAA privacy violation is any time that protected health information (PHI) is released; transferred; accessed; or divulged to an unauthorized source or entity.

A patient must give a healthcare provider authorization before the provider can disclose (release) protected health information to others. However, the provider can disclose information without an authorization for the following reasons:

1. Treatment of the individual;

   Treatment includes the management of healthcare and related services by one or more healthcare providers; including the coordination with a third party; consultations; or the referral of a patient from one provider to another.

2. To obtain payment for services rendered by the provider; and/or
3. To carry out healthcare operations.

   Examples of healthcare operations:

   - Utilization Review activities;
   - Compliance activities;
   - Internal Auditing activities; and
   - Performance Improvement activities.

The following are examples of what is allowed under HIPAA:

- Healthcare staff may orally coordinate services at the hospital nursing stations.
- Nurses or other healthcare providers may discuss a patient's condition over the phone with the patient, a provider or a family member as designated by the patient or responsible for the patient's care.
- A healthcare provider may discuss lab test results with a patient or other provider in a joint treatment area.
- The Healthcare provider may discuss a patient's condition during training rounds.

The healthcare provider is protected against certain incidental uses and disclosures as long as they have applied reasonable:

- Administrative;
- Technical; and
- Physical safeguards.

Examples of incidental disclosures:

- An unauthorized person overhears a confidential communication between providers.
- Discussion of lab results with a patient or other provider in a semi-private room.
- Disclosure to other patients in a waiting room of the identity of the person whose name is called.

Examples of HIPAA violations:

- A medical record is left open, displayed or accessible to unauthorized personnel.
- Using a white board to display patient name and diagnosis.
- A nurse viewing the lab results of a patient for which he/she has no direct involvement in the patient's care.

Providers can make disclosures, other than those previously listed, only if the patient signs an authorization. Authorizations, sometimes referred to as a consent to release, must contain certain information before the provider can disclose the PHI.

The following are the required elements which must be present on an authorization before the information can be released:

1. A description of the information to be disclosed – this description should be specific enough so the provider understands what information can be released;
2. The identification of the persons authorized to make the disclosure; In other words, the authorization should specify the name of the physician, physician group, or facility that is being authorized to disclose the information.
3. The identification of the persons or organization to whom the provider is authorized to make the disclosure. This could be a law firm, an insurance company, a patient's family member, etc.;
4. A description of each purpose of the release;
5. An expiration date or event;
6. The individual's signature and date; and
7. If signed by a personal representative, a description of his or her authority to act for the individual.

Additionally, the following required statements must be present on an authorization before information can be released:

1. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of the how the individual may revoke the authorization.
2. Treatment, payment, enrollment, or eligibility for benefits may not be conditioned on obtaining the authorization if such conditioning is prohibited by the Privacy Rule, or if conditioning is permitted, a statement about the consequences of refusing to sign the authorization.
3. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and may no longer be protected by this rule.

The patient also has many rights under HIPAA concerning their PHI (Protected Health Information). They include:

- The right to a Notice of Privacy Practices;
- The right to access and copy their PHI;
- The right to request an accounting of disclosures;
- The right to request amendments to their PHI;
- The right to request restrictions;
- The right to request how we communicate with them; and
- The right to receive notification if their information is breached.

The following are disclosures that are required by Law:

- Disclosures about victims of abuse;
- Disclosures for judicial proceedings; and
- Disclosures for Law Enforcement purposes.

If a patient requests access to their medical records, they should contact the Release of Information department.

The HIPAA Privacy Rule specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object.

If your co-worker wants information on the patient's condition, you should verify that the information is needed for them to perform their job.