HIPAA Privacy Overview

General
HIPAA stands for a federal law called the Health Insurance Portability and Accountability Act. This law, among other purposes, was created to protect the privacy and security of patient healthcare information, which is considered Protected Health Information (“PHI”). It also established uniform standards for electronic billing and the computerized transfer of healthcare information. It became effective in April 2003.

In general, the HIPAA privacy regulations provide for the following:

- It gives patients more control over their health information
- It sets boundaries on the use and release of health records
- It establishes appropriate safeguards that healthcare providers and others (i.e physicians) must achieve to protect the privacy of health care information
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients’ privacy rights, and
- It strikes a balance when public responsibility supports disclosure of some forms of patient data- for example, to protect public health

Protected Health Information
PHI includes any information (i.e. oral, recorded on paper, or sent electronically) that is unique to a patient and by itself can identify that person in regard to their physical or mental health, services rendered or payment for those services, including personal information connecting the patient to the records. Some examples of PHI include:

- Name
- Address
- Social security number
- Telephone number
- Medical record number
- E-mail address
- Hospital admission date
- Discharge date, etc.

Generally, PHI cannot be used or disclosed by staff without a patient’s consent or authorization, unless it is for “TPO”. TPO stands for Treatment, Payment and Operations.
**Treatment**- refers to how Continuum and its health care providers manage, coordinate or provide health care. This includes consulting with other health care providers or patient referrals.

**Payment**- refers to the activities necessary for Continuum and its health care providers to obtain payment for rendered services.

**Operations**- refers to the administrative, financial, legal and quality improvement activities necessary to support Continuum functions relating to treatment and payment.

---

**Notice of Privacy Practices**
The HIPAA Privacy regulations require that all patients be provided with the written Continuum Notice of Privacy Practices (“NPP”) when utilizing Continuum health services for the first time. The NPP informs patients of their rights regarding the use and disclosure of PHI as well as Continuum’s legal obligations to safeguard the PHI. Patients are asked to sign an acknowledgement form noting their receipt of the NPP. The NPP is posted on the Continuum Internet web site as well.

**Minimum Necessary Rule**
The HIPAA regulations require Continuum to take reasonable steps to limit the use and disclosure of PHI. The least amount of PHI required for you to do your job effectively is considered “minimum necessary”. Staff need to be careful in terms of how they use and share PHI. Basically, disclosure of PHI must be limited to the least amount needed to get the job done right.

**Business Associates**
Under HIPAA, when Continuum shares patient information with contracted vendors such as transcription services or billing companies, they become “business associates” and must also follow HIPAA rules. Continuum’s “business associate agreements” (contracts) with these vendors must include an acknowledgement of HIPAA compliance.

**Privacy Officer**
In accordance with the HIPAA legislation, Continuum has appointed a Privacy Officer who has overall responsibility for ensuring compliance to the HIPAA regulations. Louis I. Schenkel, the Corporate Compliance Officer, also serves as the Continuum Privacy Officer. Among his HIPAA duties are the drafting of policies and procedures. These policies are posted on the Continuum Intranet web site.

The Privacy Officer is also responsible for investigating and acting upon privacy complaints. Similar to Corporate Compliance issues, employees and others may not be retaliated against for making good faith reports of privacy violations.

Individuals also have the right to contact the Office for Civil Rights in the federal Department of Health & Human Services, which is responsible for enforcing HIPAA.

Violations of the HIPAA regulations subject violators to civil and/or criminal penalties ranging from $100 to $250,000.
If you have any questions or concerns about compliance with the HIPAA Privacy Regulations, speak to your supervisor or the Privacy Officer, who can be contacted at (212) 523-2162. If you have any questions relating to the security component of HIPAA, please contact Continuum’s HIPAA Security Officer at (212) 523-7609.

**Your Role in HIPAA**

- Ensure that PHI is not disclosed improperly
- Do not discuss PHI in elevators or in public areas such as cafeterias where your conversations may be overheard
- Protect and do not share computer passwords
- Make good faith reports of HIPAA violations to the Privacy Officer

**HIPAA Case Scenario # 1**

You work in the Medical Records Department and a certain physician requests medical records of patients that she is not involved with. Is she allowed to do this?

**Answer:**
No. Only the attending, covering or consulting physicians may have access to patient medical records. “PHI”- Protected Health Information, can only be released for the purposes of “TPO”- Treatment, Payment or Operations. Patients are entitled to expect confidentiality, the protection of their privacy and the release of PHI only to authorized parties. This physician should be reported to your supervisor or to the Corporate Compliance Officer.

**HIPAA Case Scenario # 2**

You are a physical therapist who just found out that your favorite teacher from high school is in the Emergency Department arriving via ambulance after a car accident. She had X-rays taken and her husband has asked you to get the results since you know the radiology supervisor and the Emergency Department physician is busy with another patient. Should you do this?

**Answer:**
No. Even though you have the ability to get the X-ray results, this patient’s PHI has nothing to do with your job, nor is it related to TPO. If you obtain the results from the radiology supervisor, both of you will be violating HIPAA, the Code of Conduct, and subjecting the hospital to the risk of liability for breaching the patient’s right to confidentiality and privacy.
Frequently Asked Questions

Q: Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family and friends?

A: Yes. 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. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient’s mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient’s payment options with her adult daughter.
- A doctor may instruct a patient’s roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
- A physician may discuss a patient’s treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

Even when the patient is not present or it is impracticable because of emergency circumstances or the patient’s incapacity for the covered entity to ask the patient about discussing her care or payment with a family member or other person, a covered entity may share this information with the person when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. Thus, for example:

- A surgeon may, if consistent with such professional judgment, inform a patient’s spouse, who accompanied her husband to the emergency room, that the patient has suffered a heart attack and provide periodic updates on the patient’s progress and prognosis.
- A doctor may, if consistent with such professional judgment, discuss an incapacitated patient’s condition with a family member over the telephone.

In addition, the HIPAA Privacy Rule expressly permits a covered entity to use professional judgment and experience with common practice to make reasonable inferences about the patient’s best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. For example, when a person comes to a pharmacy requesting to pick up a prescription on behalf of an individual he identifies by name, a pharmacist, based on professional judgment and experience with common practice, may allow the person to do so.
Q: Can a physician’s office fax patient medical information to another physician’s office?

A: The HIPAA Privacy Rule permits physicians to disclose protected health information (PHI) to another health care provider for treatment purposes. This can be done by fax or by other means. Covered entities (i.e. hospitals, physician offices) must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact the correct one for the other physician’s office, and placing the fax machine in a secure location to prevent unauthorized access to the information.

Q: Are health care providers restricted from consulting with other providers about a patient’s condition without the patient’s written authorization?

A: No. Consulting with another health care provider about a patient is within the HIPAA Privacy Rule’s definition of “treatment” and, therefore, is permissible. In addition, a health care provider (or other covered entity) is expressly permitted to disclose protected health information about an individual to a health care provider for that provider’s treatment of the individual.