HIPAA and Patient Confidentiality

UFHealth ST. JOHNS

UFHealth FLAGLER HOSPITAL

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

CDC.(2018). *Public Health Law.* Retrieved from https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

HIPAA Privacy Rule

The Privacy Rule standards address the use and disclosure of individuals' health information (known as "protected health information") by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities." The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used. A major goal of the Privacy Rule is to ensure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.

CDC.(2018). *Public Health Law.* Retrieved from https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

HIPAA: FEDERAL RULES TO PROTECT THE PRIVACY OF PATIENT HEALTH INFORMATION

- In April 2001, the federal government issued rules that protect the privacy of personal health information. The rules were effective in April 2003. In addition, rules were developed concerning protection of confidentiality when information is electronically transferred and rules regarding general security of health information.
- The hospital is a covered entity under the Federal Rules and must be in compliance with the rules.
- Under the Federal rules, health information includes patient's identifying data, name, address, phone number, etc. and not just medical information.

General Guidelines for Communication of Patient Information

- Patient information should NEVER be discussed in hallways, elevators, cafeterias or other public areas and should never be shared with persons not directly involved in that patient's care and treatment.
- Verbal reports of clinical information should only be given to the patient by authorized medical personnel directly involved in the patient's care and treatment.
- Adhere to appropriate computer access and data authorization requirements as outlined in appropriate policies when documenting patient information in the EMR.
- Patient medical information should not be left on an answering machine, as the message may be accessed by individuals other than the intended recipient.
- Transfer of patient information via fax machines should only be done by authorized medical personnel, such as when a patient's condition warrants emergency communication.

Confidentiality and Security of EMR Patient Health Information

- Individuals permitted access to UF Health Flagler Hospital computer information systems and/or other sources of confidential information are required to sign a Confidentiality and Security agreement.
- The IDs and passwords used to access computer information are confidential and should not be posted, shared or distributed to anyone other than assigned user per required policies.
- *EMR users may not access information of family members, friends or other individuals for non-work related purposes even if written or oral patient authorization has been obtained. Users designated as a medical power of attorney or healthcare surrogate should submit a formal request through the Health Information Department.*

Allowed Uses and Disclosures of Patient Information

- Prior to treatment, the hospital must obtain consent for the use and disclosure of Patient Information (PI). Consent is not required during emergency treatment; however, consent must be obtained as soon as possible after the emergency treatment. Hospital personnel must document in the EMR any failed attempts to obtain consent.
- The patient has the right to request restrictions on the use and disclosure of PI, but the hospital does not have to agree to the request. If the hospital agrees, the restriction is binding. Such agreements can only be made by those authorized to do so.
- Prior to obtaining consent, the hospital must give the patient a copy of our Notice of Health Information Processes. This notice provides examples of the ways health information may be used and disclosed.

Allowed Uses and Disclosures of Patient Information continued

- Together, the Notice of Health Information Processes and the consent allow the hospital to use and share information with its own staff and with physicians, home health agencies, nursing homes, other hospitals and other types of health agencies as part of the patient's care. A special authorization is required to release information regarding psychiatric treatment and the patient must specifically agree to be listed in the hospital's patient directory.
- The consent also allows the hospital to use and disclose PI for billing, and payment, and to disclose PI to outside contractors (such as transcriptionists), but the hospital must obtain an agreement from such "business associates" to keep all PI confidential.
- Consent is not required to disclose information to law enforcement, medical examiners, or Agencies when required by law (such as child abuse reporting, or reporting of infectious disease to the Health Department).
- Even with consent, the rules require that only the minimum necessary information be disclosed. Physicians, hospital staff and students have restricted EMR access to patient information of patients under their direct care. In additional, some hospital personnel may have further restrictions regarding specific areas of the EMR.

Examples of How Patient Information Can be Used and Disclosed

Physicians, hospital staff, and students:

- may have access to see and use patient information in order to participate in the patient's care and treatment or as part of necessary hospital operations required by their healthcare role.
- may disclose PI to other physicians, hospital staff, and students who are also involved in the patient's care at the hospital, or who will be providing follow-up care after hospital treatment.
- may disclose PI to a patient's authorized representative, such as health care proxy or health care surrogate.
- ***may NOT disclose PI to co-workers not involved in a patient's care, or to your own family and friends, to physicians and other practitioners not involved in a patient's care, or to any other person or entity unless authorized to do so.***

Breaches of Patient Confidentiality

Students who have a reasonable basis to believe that a breach of patient confidentiality has occurred should report an incident(s) as soon as possible to any of the following:

- School Student Coordinator
- Human Resources Department
- UF Health Flagler Hospital or School Administrator

Penalties for Unauthorized Use and Disclosure of Patient Health Information

Unauthorized Use and Disclosure of a Patient's Health Information is a Criminal Offense Punishable by a Fine (Up to $50,000), Imprisonment (Up to 10 Years), or BOTH and May Result in Immediate Termination.

References for Additional Reading

- UF Health St. Johns Policies:
  - I-HIM-Uses & Disclosures of Protected Health Information
  - I-HIM-Request for Restriction of Protected Health Information