HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was established in 1996 to improve the security of the storage and use of health care data.  These regulations define how health care agencies must secure patients’ personal information and regulate its disclosure.

IT staff members should understand how HIPAA applies to their work so they can correctly handle sensitive information and demonstrate the organization’s compliance with the law in order to protect patients and the organization (DNS Stuff, n.d.).  Unauthorized access or release of data can lead to problems for the individuals whose data has been compromised and also fines and penalties for organization (Ashraf, n.d.).  Two important IT-related aspects of HIPAA are the Privacy Rule and the Security Rule.

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients specific rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections (HHS, "Privacy Rule," n.d.).

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral (HHS, "Summary of the HIPAA Privacy Rule," n.d.). The Privacy Rule calls this information "protected health information (PHI)."  PHI is information, including demographic data, that relates to:

* the individual’s past, present or future physical or mental health or condition,
* the provision of health care to the individual, or
* the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual, such as name, address, birth date, Social Security number).

HIPAA Security Rule

The Security Rule (HHS, "Summary of the HIPAA Security Rule," n.d.). requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting **electronic personal health information** (ePHI). Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

Note that the concept of personal health information is very similar to the term **personally identifiable information** (PII), which is a broader term used by the federal government to indicate "any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; an any other information that is linked or linkable to an individual," such as medical, educational, financial, and employment information (GAO, 2008).

References

Ashraf, A. (n.d.). PII and PHI overview: What CISSPs need to know. Infosec. https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/asset-security/protecting-privacy/#gref

Department of Health and Human Services (HHS). (n.d.). The HIPAA privacy rule. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Department of Health and Human Services (HHS). (n.d.). The HIPAA security rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

DNSStuff. (n.d.) What is HIPAA compliance? https://www.dnsstuff.com/what-is-hipaa-compliance

United States Government Accountability Office (GAO). (2008). Privacy: Alternatives exist for enhancing protection of personally identifiable information. https://www.gao.gov/new.items/d08536.pdf