

HIPAA

Health Insurance Portability & Accountability Act of 1996

PRIVACY RULE OVERVIEW

The **Health Insurance Portability and Accountability Act (HIPAA)** is a complex legislative act with four primary aspects – privacy being just one.

National standards to protect individual medical records and other **protected health information (PHI)** were established for the first time. [Compliance Date: April 14, 2003]

Providers (e.g. hospitals, nursing facilities, HMOs, Physicians' Offices, etc.) are referred to as **covered entities (CEs)** which conduct certain health care transactions electronically. Health plans (e.g. Blue Cross/Blue Shield, Medicare, private health insurances, etc.) and health care clearinghouses are also covered entities. *[FYI – although MVCC collects certain protected health information the College is not a covered entity]*

Provider Activities:

- Notification of Privacy Practices explaining to patients* uses/disclosures of their own PHI and other rights.
- Adopting and implementing privacy policies and procedures.
- Training all employees regarding the policies and procedures.
- Providing security for any/all records containing individually identifiable health information.
- Selecting a Privacy Officer who will be responsible for assuring that all policies and procedures are adopted and followed on an on-going basis.

*Patients may also be referred to as clients, residents, and/or consumers.

Covered entities (CEs) may use/disclose protected health information (PHI) for its own **treatment, payment and healthcare operations (TPO)** without patient authorization. Healthcare operations include, as examples, performance/quality improvement activities and training of healthcare professionals. CE's cannot sell PHI to a **Business Associate** (a **BA** is a person/entity that performs functions that involve the use/disclosure of PHI on behalf of, or provides services to, a CE) or any other third party for its own purposes. CE's cannot sell lists of patients or enrollees to third parties without each person's authorization. CE's may disclose PHI without authorization for some public health purposes, e.g. vital statistics, child abuse/neglect, etc. To limit access to Minimum Necessary, CE's must evaluate practices and enhance safeguards to limit unnecessary or inappropriate access to or disclosure of PHI.

Reasonable Privacy Safeguards must be utilized to protect against uses/disclosures not permitted by the Privacy Rule. The following listing is just an example of some of the safeguards:

- Isolate or lock medical records and other PHI in cabinets or rooms.

- Avoid using patients' names in public places, e.g. hallways, elevators, cafeteria, nursing stations, etc.
- Post signs and in-service employees and the medical staff regarding patient confidentiality.
- Speak quietly and be aware of who is around you when speaking to a patient (in a non-private setting) or his/her family members about the patient's condition.
- Isolate computer screens containing patient information from public view.
- Use additional computer security safeguards, e.g. passwords, restricting access by time of day and/or location, etc.
- Restrict access to PHI to a "need to know" basis.

Patients are enabled to find out how their information may be used and must also be provided, upon request, an accounting of disclosures. A patient has the right to examine and receive a copy of their own medical record(s) and may make amendments to their own health information. Legally authorized personal representatives (e.g. legal guardians, empowered health care agents – NYS specific, healthcare power of attorney) must be treated as the individual (except as otherwise provided) with respect to PHI uses/disclosures/rights. [Note: all forms of Power of Attorney and the Health Care Agent/Proxy are voided upon the patient's death.]

CEs may be held accountable if violations of a patient's' right to privacy occurs. Civil and criminal penalties can be imposed. **Students must NOT remove and/or disclose any protected health information; check to make sure that all patient identifying information is redacted. Unintentional or intentional disclosure of PHI will result in a student's dismissal from their program of study; e.g. Nursing, Nursing, Health Information, etc.**

The Notice of Privacy Practices must be provided at the first treatment after the compliance date. The Notice must include, in plain language, the individual's rights related to PHI and how they may exercise their rights including how to complain to the CE. Who to contact for additional information about the CE's privacy policies must be stated. The CE's uses and disclosures of PHI and a statement that the CE is required by law to maintain PHI privacy must also be included. CEs must make a good faith effort in obtaining written acknowledgement of receipt of the Notice.

Words of Caution: The Privacy Rule does not replace Federal, State or other laws granting individuals greater privacy protections. It will be very important to keep abreast of all applicable laws, rules and regulations. Visit the following Web site for more information: www.hhs.gov/ocr/hipaa/

Sources: PRG Quick Notes: HIPAA Privacy Basics
 Journal of AHIMA, Practical Advice on HIPAA Policies, Procedures, April 2003