Protecting Privacy of Patient’s Health Information

1. **Information Required to be Protected**: The privacy of all medical records, billing records, and other individually identifiable health information must be protected.

2. **Boundaries on Health Information Use and Release**: With few exceptions, an individual’s health information can be used for health purposes only.
   1. Ensure that health information is not used for non-health purposes. Patient information can be used or disclosed only for purposes of health care treatment, payment, and operations. Health information cannot be used for purposes not related to health care without explicit authorization from the individual. Thus, for example, a health plan is not permitted to access the personal health information held by the plan for employment-related purposes, unless the health plan first obtains the authorization of the patient.
   2. Provide the minimum amount of information necessary. Disclosure of information must be limited to the minimum necessary for the purpose of the disclosure.

3. **Ensuring the Security of Personal Health Information**: The regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity. In this way, implementation of the standards will be flexible and scalable, to account for the nature of each entity's business, and its size and resources. Covered entities must:
   1. Adopt written privacy procedures. These must include who has access to protected information, how it will be used within the entity, and when the information would or would not be disclosed to others. They must also take steps to ensure that their business associates protect the privacy of health information.
   2. Train employees and designate a privacy officer. Covered entities must provide sufficient training so that their employees understand the new privacy protections procedures, and designate an individual to be responsible for ensuring the procedures are followed.
   3. Establish grievance processes. Covered entities must provide a means for patients to make inquiries or complaints regarding the privacy of their records.

4. **Penalties for Misuse of Personal Health Information**: There are penalties for covered entities that misuse personal health information.
   1. Civil Penalties. Covered entities that violate these standards would be subject to civil liability. Civil money penalties are $100 per incident, up to $25,000 per person, per year, per standard.
   2. Federal criminal penalties. There would be federal criminal penalties for covered entities that knowingly and improperly disclose information or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information under “false pretenses”; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.
5. **Disclosure of Health Information That Do Not Require Patient Authorization:**
   Within certain guidelines found in the federal privacy standards, covered entities may disclose certain types of information without patient authorization; these types of information are listed below. The federal privacy standards permit, but do not require, these types of disclosures. If there is no other law requiring this information to be disclosed, a covered entity will still have to make judgments about whether to disclose this information, in light of its policies and ethical principles. If you have any question regarding whether a particular disclosure requires patient authorization, please do not hesitate to ask your manager.
   1. Oversight of the health care system, including quality assurance activities.
   2. Public health.
   3. Research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board.
   4. Judicial and administrative proceedings.
   5. Limited law enforcement activities.
   7. For identification of the body of a deceased person, or the cause of death.
   8. For facility patient directories.
   9. For activities related to national defense and security.

6. **Information Regarding the Federal Privacy Standards:** Visit Health Human Services - Office of Civil Rights web site to learn more about the federal privacy standards.