Protecting the Privacy of Patients' Health Information

Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, individually identifiable health information held by covered entities and their business associates is covered by certain federal protections. The Privacy Rule also permits the disclosure of health information needed for patient care.[1]

Patient Protections

Patients have the right to access their medical records and other health information. Requests for copies must be fulfilled within 30 days.[2] Patients may dispute incorrect or missing information; the file should be updated within 60 days.[2] By law, a patient's health information can be used and shared for specific reasons not directly related to the patient's care. This is to ensure that good care is provided by physicians, to make sure nursing homes are safe and clean, or to report when influenza is in your area. Patients have the right to know how their health information is being used and shared by their doctor or health insurer. They also have the right to request that certain information from their medical record not be shared.[2]

The federal government has also created the HIPAA Security Rule, which requires specific protections be made to ensure the safety of a patient's electronic health record (EHR). Certain measures, including access controls (eg, passwords, PIN numbers), data encryption, and an audit trail, are built into EHR systems. Federal law also requires that health care providers notify patients in the event of a possible information breach.[3]

Provider Information

Although the Privacy Rule provides for certain protections to personal health information, it is balanced to ensure that information needed for patient care is available when necessary.[4]

Who Must Comply With the Privacy Rule?

All HIPAA-covered entities are required to comply with the rule.[5]