Recently, the first-ever federal privacy standards to protect individuals' health-care information went into effect. The mandate for these standards, collectively known as the Privacy Rule, was in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The Privacy Rule gives individuals access to their medical records and greater control over the use and disclosure of their personal health information. States are still free to keep or adopt their own policies or practices that are at least as protective as the new federal requirements.

Who Is Covered

Entities subject to the Privacy Rule include health-care providers, health plans (including insurance companies and HMOs), and health-care clearinghouses, such as physicians' billing services. The regulations also apply to “business associates,” meaning any organization or person (other than a worker for a covered entity) that receives or accesses private medical information on behalf of a covered entity. When a covered entity uses a business associate, the two must enter into a written agreement containing specific protections for the health information used or disclosed by the business associate.

On its face, the Privacy Rule does not directly apply to employers, but that is not to say that employers need not become familiar with its requirements. Employers frequently interact with covered entities and their business associates. In addition, employers administering their own group health plans are effectively brought within the reach of the Privacy Rule.

Safeguards for Individuals

The Privacy Rule applies to “protected health information” (PHI), defined as all individually identifiable health information held or transmitted in any form or media, whether electronic, paper, or oral. Individuals generally should be able to see and obtain copies of their PHI within 30 days of a request. Covered entities must provide a notice to individuals describing how their PHI may be used and informing them of their rights under the Privacy Rule.

In the interest of promoting quality health care, providers are not restricted in their ability to share information needed to treat patients. Generally, PHI may not be used for purposes unrelated to health care. However, in the rare cases where it is allowed, only a minimum amount of protected information may be used or shared. Covered entities may release medical information to outside businesses such as insurers, banks, or marketing firms only with specific written authorization from the individual.

The Privacy Rule gives individuals the right to request alternative means or locations for receiving PHI communications. For example, a patient could ask a doctor to communicate with the patient through a designated telephone number or address. Another reasonable accommodation might be sending medical information to a patient in a closed envelope rather than on a postcard.

Policies and Procedures

The Privacy Rule requires covered entities to set up policies and procedures to protect the confidentiality of PHI. Written privacy procedures must identify staff with access to PHI and describe how such information will be used and when it may be disclosed. There must be training of employees in privacy procedures and designation of an individual to be responsible for insuring that those procedures are followed.

Covered entities may continue existing disclosures of health information for certain public responsibilities, subject to limits and safeguards that are specific to such circumstances. Examples include emergencies, identification of the body of a deceased person, and public health needs. If there is no other law that mandates disclosure to meet a particular public responsibility, covered entities may use their professional judgment to decide whether to make disclosures.

Enforcement

The Government may impose civil penalties of $100 for each failure to comply with a Privacy Rule requirement. A penalty may not exceed $25,000 per year for multiple violations of the same requirement in a calendar year. If a violation is due to reasonable cause, involved no willful neglect, and is corrected within 30 days of when an entity knew or should have known about it, no civil penalty may be imposed. A knowing violation of the Privacy Rule could also bring a fine of $50,000 and up to a one-year prison term. Maximum criminal penalties are higher if the wrongful conduct involves false pretenses, or use of the health information for commercial advantage, personal gain, or malicious harm.

Advance Medical Directive Updated

To reflect the change in the law discussed in this article, we updated the Advance Medical Directive prepared for our clients. Please contact us if you would like to revise or update your Advance Medical Directive.