Back to HIPAA Basics: What Is Protected Health Information?

June 10, 2013

As the September 2013 compliance date for the Omnibus HIPAA regulations approaches and the Office of Civil Rights settlement announcements continue, more organizations are assessing risks and implementing a more comprehensive HIPAA compliance strategy. For many organizations, this process begins with a simple question: to what extent do we create or maintain protected health information?

For many people, the phrase protected health information or PHI is associated with medical record documentation. But the definition under HIPAA is much broader. Protected health information is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium, but not including employment records or education records. Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual that 1) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of healthcare to an individual and 2) identifies that individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

The classification of information as protected health information is, therefore, dependent on the purpose for which it was collected. Once obtained, the information remains protected health information so long as it remains identifiable. Separation or segregation of demographic or financial information from the health services to which it relates does not remove the information from the category of protected health information. For example, if an individual writes a check or submits credit card information to a healthcare provider to pay for a healthcare service, the check or credit card information becomes protected health information. Storage of this information in a database that is separate from the practice management or electronic medical record system that describes the health care service does not affect its classification as protected health information.

A covered entity or business associate may only use or disclose protected health information as permitted or required by HIPAA. Further, covered entities and business associates are required to implement certain safeguards to maintain the confidentiality, security, and integrity of protected health information. Covered

entities include health plans, health care clearing houses, and health care providers who engage in certain electronic transactions. Business associates are individuals and entities who receive, create, maintain or transmit protected health information on behalf of a covered entity related to a function or activity regulated by HIPAA, or as part of the provision of legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for the covered entity or an organized healthcare arrangement in which the covered entity participates.

So what does this mean?

- Are an individual's address, phone, Social Security number, and other demographic information maintained by a hospital protected health information?

  It depends. If the records are maintained on a patient related to the provision of service in the hospital, then yes, they are protected health information. If, however they are maintained on an employee related to a pre-employment health screening, then they are not.

- Is a law firm required to provide HIPAA protections to patient medical records it obtains in the representation of a client?

  It depends. If the records were obtained from a physician client for the purpose of defending a peer review proceeding or from a health plan to determine coverage of a procedure for a beneficiary, then yes, the law firm is acting as a business associate and is responsible for HIPAA compliance related to the records. If, however, the records were obtained pursuant to an authorization signed by the patient to defend a client in a personal injury action, the records are protected health information, but the law firm did not obtain them as a business associate.

- Does a bank become a business associate when it establishes an account for a health care entity?

  It depends. If the bank solely processes financial transactions for the client, then no, its activities are exempted from HIPAA. If, however, the bank also offers services related to accounts receivable, it may trigger the definitions under HIPAA and become a business associate.

If a company maintains protected health information as a covered entity or business associate, it must implement policies, procedures, and adequate safeguards to protect the information in order to comply with HIPAA. In addition to the proactive, risk management requirements for HIPAA, understanding whether your organization is responsible for HIPAA compliance related to protected health information is necessary in the event of a breach to that information. Where the security or confidentiality of protected health information in the possession or control of a covered entity or business associate, certain notifications are mandated under HIPAA. These requirements are in addition to state law requirements for data breach.

Identifying and understanding the data in your organization is the first step to ensuring HIPAA compliance and overall best practices for information security. Once the scope of information is understood and its location is identified, your organization can begin assessing and prioritizing steps needed for adequate protection.

If you have any questions about how these privacy and security requirements affect your company, please contact your Lathrop Gage attorney or any of the attorneys listed above. For more cutting edge insights, news, and commentary, visit our Media, Privacy & Beyond blog at http://www.media-privacy.com.