BROOKS PIERCE

Could Your Law Firm Unknowingly Be a HIPAA Business Associate?

05.04.2011

Since 1996, the Health Insurance Portability and Accountability Act (HIPAA) has affected nearly every aspect of health care. HIPAA imposes an array of measures aimed at keeping personal medical information private and secure. Its provisions can apply to law firms and attorneys in their everyday representation of certain clients. Because of HIPAA's stiff penalties and other potentially embarrassing consequences, anyone working with clients in health-related fields must understand their duties under HIPAA.

It starts with "covered entities"

HIPAA applies to covered entities, which are (1) health plans, (2) healthcare clearinghouses, and (3) healthcare providers that conduct certain transactions in an electronic form. The definition for each of these types of covered entities is very technical. For example, covered entities can include group health plans, except certain small, self-administered plans. Also included are hospitals, doctors, and clinics but only if they conduct certain transactions in an electronic form. Those transactions include requests to obtain payment, requests for health care, transmissions of patient information, and communication between a healthcare provider and health plan regarding benefits, coverage, and similar items. Whether or not an entity is a covered entity can be a close question—anyone representing health-related organizations must determine whether their clients are covered entities.

Lawyers and firms can be "business associates" under HIPAA

People or entities that perform certain functions for a covered entity involving protected health information (PHI) are called business associates. Business associates can provide legal, actuarial, accounting, and consulting services. The Department of Health and Human Services (HHS) has explicitly stated that an attorney whose legal services to a health plan involve access to PHI is a business associate. This could be a business attorney planning a sale of a medical business, a healthcare attorney answering day-to-day questions about patient information for a hospital or doctor, or a litigator helping an insurance company through litigation regarding patient coverage.

Business associates are directly subject to HIPAA's privacy rules, security rules, enforcement provisions, fines, and penalties. Further, recent guidance from HHS would consider subcontractors to business associates as business associates under HIPAA. 75 Fed. Reg. § 40,868. This could include law firms that are subcontractors to business associates.

Business associates must report certain breaches of unsecured or unencrypted PHI, abide by a business associate agreement, and account for certain disclosures of PHI. Disclosures of PHI in violation of HIPAA may need to be reported to the covered entity, government authorities (federal and state), and affected individuals, which can result in significant embarrassment, costs, and fines.

Business associates must have "business associate agreements"

Business associates must have a written business associate agreement (BAA) with the covered entity, and recent proposed guidance requires a business associate to have a BAA with subcontractors they hire. 75 Fed. Reg. § 40,868.

Thus, a law firm and the covered entity for which it works need a BAA. For example, if a law firm, as a business associate, hired a document scanning company to help with document management of HIPAA-covered documents, the law firm might need a BAA with the scanning company. A law firm working only for a business associate may also need a BAA.

A BAA details the relationship between the two entities. For example, a BAA describes permitted or required uses of PHI, prohibits use of PHI except as required by the agreement or by law, and requires appropriate safeguards to prevent a use of PHI other than as provided for by the BAA. Where one party knows of a material breach or violation by the other under the BAA, that party is required to take reasonable steps to cure the breach or end the violation. If those steps are not successful, the party with the knowledge of the breach must terminate the BAA.

Business associates need extensive security policies for EPHI

Business associates must create and implement administrative, physical, and technical safeguards for electronic PHI (EPHI), which is PHI created, stored, transmitted, or received electronically. Business associates must develop and enforce related policies, procedures, and documentation standards. For a law firm, this can require creation of a building security policy, computer security policy (encryption, security monitoring, password safety), safety and password protection for EPHI stored on firm computers, attorney and staff training, appointment of a security officer to oversee all HIPAA compliance, and periodic review of the all of the above. The periodic review must be made in reference to the changing technology, evolving computer threats, and HHS's annual guidance regarding security. Any security policy must be drafted in conjunction with a firm's information technology and administrative staff, along with HIPAA-knowledgeable attorneys. The goal of the security policy is to prevent the breach of unsecured EPHI because HIPAA requires special reports for breaches of unsecured (unencrypted) EPHI.

HIPAA's requirements to prevent disclosure of PHI are extensive and evolving. Those working with health-related clients must keep informed to ensure they are meeting HIPAA's requirements.