

HIPAA – Understanding the basics of “PHI”

Privacy in the health industry has become a mandatory standard applied by all physicians in America. With the rising concern of clients' privacy being at stake, the US Department of Health and Human Services ("HHS") issued a Privacy Rule in 1996 that has changed the way physicians operate their practice.

HHS implemented the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which addresses the disclosure of patients' health information, also referred to as "protected health information, or "PHI," by those organizations that are subject to the rule ("covered entities"). It further addresses the standards applied in which patient's health information is to be used.

One of the primary objectives of the privacy rule is to provide individuals with the assurance that their health information is protected and not being distributed without their knowledge and/or approval by the covered entities.

Who are the covered entities?

Covered entities under HIPAA are groups that include health plans, healthcare clearinghouses, and any healthcare provider that transmits health information. In addition to the covered entities, HIPAA also regulates against non-covered entities, such as "business associates" and "trading partners." Business associates are those who assist or perform functions for the covered entities, and trading partners are those that transmit health information in standardized electronic form for the covered entities.

Pursuant to HIPAA, every covered entity involved in an agreement with a business associate or a trading partner must enter into a contract, called a "Business Associate Agreement," or "Trading Partner Agreement," outlining the following:



- a description of the allowable uses and disclosures of the health information;
- an agreement that PHI will accessible by patient for inspection, amendment and accounting;
- an agreement that a business associates' books and records related to it's functions performed are accessible to HHS, if needed.
- requirement that PHI related to the covered entity be either destroyed or returned to the covered entity at the time of termination of the contract.

As most medical practices are pressed for time, many fail to take the proper actions to ensure they're practicing and applying the law appropriately. The following is a list of steps covered entities can use to help avoid noncompliance issues with HIPAA:

1. Ensure the staff understands the importance of privacy.

Pursuant to HIPAA regulations, it requires every practice to have written security policies and procedures in place. It is advised to always go over these policies with your staff on a periodic basis. The importance of this cannot be emphasized, as the majority of breaches occur within the practice through errors of the staff. Make sure your staff is properly trained on HIPAA-related requirements and practices.

2. Ensure policies and procedures are updated.

With the rules constantly changing, it is advised to review the current policies and procedures with an attorney to make sure they are up-to-date. Ensure all your HIPAA-related policies and procedures are updated and compliant with the current laws.

3. Conduct a Formal Risk Analysis.

HIPAA further requires all covered entities to periodically conduct a formal risk analysis. In addition, covered entities are also required to formally evaluate their program to ensure HIPAA compliance and compliance with recent changes such as the HITECH Act. If this has not been completed, make sure to consult with an attorney and make the changes to your policies and procedures as necessary.

4. Understand the business relationship with third-parties.

HIPAA further requires for practices to obtain assurances from their business associates that they will implement the necessary safeguards to protect the confidentiality, integrity and availability of the electronic health information they create, maintain or transmit on behalf of the practice. The primary point is to always know the business associate, as every entity a practice works,





or shares information with, is essentially an extension of the practice.

Ensuring compliance with HIPAA has recently drawn more attention as the Office for Civil Rights began conducting HIPAA compliance audits in November 2011. No matter the busy schedules medical practices have, taking the time to sit-down with an experienced attorney will pay dividends, and most importantly it will protect one from non-compliance with the law. Rather than taking a reactive approach, it may be prudent to be proactive and begin to install protections that will allow you to detect and prevent trouble down the road.

"An ounce of prevention is worth a pound of cure."

Adil Daudi is an Attorney at Joseph, Kroll & Yagalla, P.C., focusing primarily in Health Care Law, Fraud and Abuse, Regulatory Compliance, Asset Protection, Physician Contracts and Employment Agreements, Medical/Corporate Formations, Estate Planning, Shariah Estate Planning, and Non-Profit Organizations. He can be contacted for any questions related to this article or other areas of law at adil@josephlaw.net or (517) 381-2663.



DEDICATED. DETERMINED. DEPENDABLE.