

EMPLOYERS WHO FAIL TO PROTECT THEIR EMPLOYEES' HEALTH INFORMATION FACE THE RISK OF CIVIL AND CRIMINAL PENALTIES

By Mark E. Abraham

Health care providers are not the only entities who must comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Under the privacy regulations (the "Privacy Rule"), an employer or any business that *maintains its own individual or group health plan* must have written agreements with certain individuals or organizations with which it does business ("Business Associates") governing the use and disclosure of protected/personal health information ("PHI") (defined below). The Privacy Rule does not displace federal or state laws that grant individuals broader privacy protections but instead seeks to provide a foundational set of protections for patients' medical information.

Who is Covered under the Privacy Rule?

Under the Privacy Rule, a "Covered Entity" includes (1) certain individual or group health plans, (2) health care clearinghouses, and (3) health care providers who transmit PHI in electronic form. If you are an employer and you have an individual or group health plan that provides or pays the cost of medical care, you are a Covered Entity and must comply with the Privacy Rule. Health plans include employer-sponsored group health plans, government and church-sponsored health plans and multi-employer health plans. A group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not considered a Covered Entity. Covered Health plans also include health, dental, vision, and prescription drug insurers, HMO's, Medicare, Medicaid, and long-term care insurers.

What is PHI?

PHI is defined broadly as all "individually identifiable information" in any form, electronic or non-electronic, that is held or transmitted by a covered entity, including oral communication. Individually identifiable information is information that is created or received by a health care provider, health plan, employer, or health care clearinghouse and relates to the past, present, or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment for health care to an individual. Individually identifiable health information also includes demographic information collected from an individual that identifies an individual (or could reasonably be used to identify an individual) such as an individual's name, address, birth date, or Social Security Number.

Employment records are specifically excluded from the definition of PHI. Therefore, records created, received, or maintained by a covered entity *in its capacity as an employer* are not covered by the Privacy Rule (e.g., fitness-for-duty evaluations, drug screening results, sickness and disability leave requests, and documents needed to comply with the Americans with Disabilities Act, workers' compensation laws, and the Family Medical Leave Act). However, any PHI created, received, or maintained by a covered entity *in its capacity as sponsor of a health care plan*, acting on behalf of the health plan, is subject to the Privacy Rule.

Definition Of A "Business Associate"

HIPAA defines a "Business Associate" as a person who or an entity that:

- (a) On behalf of a covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing or:
- (b) Provides legal, actuarial, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a Covered Entity.

This article appeared in the Fall 2006 issue of the GR Review.

EMPLOYERS WHO FAIL TO PROTECT THEIR EMPLOYEES' HEALTH INFORMATION FACE THE RISK OF CIVIL AND CRIMINAL PENALTIES (CONTINUED)

A Business Associate contract is required whether a Business Associate's use of PHI or a covered entity's disclosure of PHI is momentary, temporary or long-term, whether the disclosure occurs on the covered entity's premises or elsewhere, regardless of whether the Business Associate will store PHI or immediately destroy it.

Business Associate Agreement

Covered entities may disclose PHI to a Business Associate only after receiving satisfactory assurance that the Business Associate will safeguard the information. A Covered Entity must enter into contracts with its Business Associates that will protect the confidentiality of PHI when such information is created, received, used by or disclosed by the Business Associates. The contract between the Covered Entity and the Business Associate, known as a "Business Associate Agreement," must, among other requirements, establish the permitted and required uses and disclosures of PHI by the Business Associate and ensure that any agents and subcontractors to which the Business Associate provides PHI on behalf of the Covered Entity also agree to the same restrictions and conditions that apply to the Business Associate with respect to the information. Generally speaking, the Business Associate must give certain assurances to the covered entity that (1) the Business Associate will not use or disclose PHI other than as permitted by the agreement or required by law; (2) the Business Associate will use appropriate safeguards to protect the confidentiality of PHI; (3) the Business Associate will report to the Covered Entity any use or disclosure not permitted by the agreement; and (4) the Business Associate will ensure that its agents or subcontractors will agree to the same restrictions as those placed on the Business Associate by the agreement. The Business Associate Agreement must also describe what is to be done with the PHI upon termination of the relationship between the Covered Entity and the Business Associate.

Penalties For Failure To Comply With HIPAA's Privacy Rule

HIPAA provides for civil and criminal penalties for violations of the Privacy Rule on "...*any person* who violates a provision... [of the Privacy Rule]." Even if done by a Business Associate, any such violation will be attributed to the Covered Entity if it knew of the wrongful conduct and failed to take corrective action or prevent the wrongful conduct. Civil penalties can include up to a maximum \$25,000 annual fine *per violation* of a single standard per year. Criminal penalties can include up to a maximum \$250,000 fine and a ten year prison term.

Conclusion

It is important to ensure that a Business Associate agreement is in place, where necessary, and that the Privacy Rule protecting an employee's health information is taken seriously as the penalties for non-compliance are severe. If you have any questions, please feel free to contact me or the attorney with whom you regularly work at Gould & Ratner.

Mark Abraham is an Associate in Gould & Ratner's Litigation Group. He may be reached at 312.899.1601 or via email at mabraham@gouldratner.com.

This article appeared in the Fall 2006 issue of the GR Review.