Cooley

February 17, 2010

The American Recovery and Reinvestment Act of 2009 is commonly known for its provisions designed to stimulate a flagging economy. However, the Act's Title XIII (known as the "Health Information Technology for Economic and Clinical Health Act" or "HITECH Act") has another purpose—to impose obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") directly on business associates (as defined under HIPAA) with respect to the way they handle certain health-related information in connection with an employer's health plan and to impose civil or criminal penalties for any violations of those obligations. This *Alert* discusses how business associates are affected by the HITECH Act and what employers should do to monitor the compliance of business associates under the HITECH Act.

## HIPAA in brief

As described in a prior *Alert*, HIPAA mandates that a "covered entity" possessing "personal health information" ("PHI") comply with certain privacy and security requirements in order to maintain the confidentiality and security of PHI. A covered entity is a health care provider, health care clearinghouse or health plan. For this purpose, a "health plan" includes insured and self-insured group health plans and HMOs, flexible benefit plans with medical savings accounts, employee assistance plans and wellness benefit programs. An employer that sponsors a health plan is not a covered entity. However, such an employer may still be affected by HIPAA in two ways.

First, as a health plan sponsor, the employer is responsible for the health plan's compliance with HIPAA. Accordingly, the employer must determine how the plan should comply with HIPAA and ensure that it does so comply. In carrying out its responsibilities under the plan, an employer may delegate some or all of those responsibilities to business associates, but the employer remains ultimately responsible for the plan's HIPAA compliance. A business associate is a third party entity that either (i) on behalf of a covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of PHI or (ii) provides services to a covered entity that involve the disclosure of PHI by the covered entity or its business associates. Often, an employer sponsoring a self-funded health plan or a health flexible spending account ("health FSA") will enter into a business associate agreement with a third party administrator to process benefit claims or requests for reimbursement from the health plan or health FSA.

Second, if the employer sponsoring a health plan performs certain plan administrative functions (*e.g.,* reimbursing health care expenses or deciding health benefit appeals), the employer likely will have access to PHI obtained from the health plan. In that case, the employer itself must comply with HIPAA's privacy and security requirements as a condition to receiving PHI from the health plan.

Accordingly, in conducting its operations involving health benefits, a covered entity and an employer sponsoring a health plan often will make use of third parties that may be "business associates" of the covered entity.

## HIPAA after the HITECH Act

Until the HITECH Act, a business associate's obligations under HIPAA, if any, were only those passed through to the business associate in a business associate agreement with the covered entity. The HITECH Act changes this indirect obligation to a direct one by imposing obligations under HIPAA's privacy and security rules directly on business associates, meaning that business associates, without regard to the provisions of their business associate agreements with covered entities, must now comply with the use and disclosure requirements designed to preserve the privacy of PHI, meet certain administrative, physical, and technical security requirements and put in place policies, procedures, and documentation relating to such security requirements.

In addition, business associates have a new obligation to provide notification to a covered entity following discovery of a breach of unsecured PHI, identifying each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during the breach. Such notification must be made without unreasonable delay, but in no case later than 60 days after the business associate's discovery of the breach.

State and federal authorities now have increased authority to pursue a business associate for a HIPAA violation

and to seek the imposition of greater civil and criminal penalties.

### Action steps for covered entities

An employer with a health plan that uses the services of one or more business associates should confirm that each business associate providing services to the health plan is aware of its enhanced HIPAA obligations, which became effective February 17, 2010. Such confirmation may already have been obtained by the plan's insurer or third party administrator, but if it has not, communication with the business associate is advised. An employer might also consider seeking an acknowledgement that the business associate is in full compliance with its enhanced obligations under HIPAA. View a sample acknowledgement letter.

If you have questions about this *Alert,* please contact one of the attorneys listed above.

### Circular 230 Disclosure

The following disclosure is provided in accordance with the Internal Revenue Service's Circular 230 (31 CFR Part 10). Any tax advice contained in this *Alert* is intended to be preliminary, for discussion purposes only, and not final. Any such advice is not intended to be used for marketing, promoting or recommending any transaction or for the use of any person in connection with the preparation of any tax return. Accordingly, this advice is not intended or written to be used, and it cannot be used, by any person for the purpose of avoiding tax penalties that may be imposed on such person.



# Key Contacts



| | |
|---|---|
| Tom Reicher<br>San Francisco | treicher@cooley.com<br>+1 415 693 2381 |