Montgomery & Hansen LLP

Client Alert June 1, 2011

New Privacy Rules for Technology Companies Doing Business with Health Care Providers

Technology companies that provide services to health care providers, health care clearinghouses or health plans must comply with two significant federal laws and the regulations implementing those laws by the Department of Health and Human Services ("HHS"). Failure to do so may result in significant civil and criminal penalties.

Technology companies increasingly provide online services to health care providers, health care clearing houses and health plans. Those services often include collecting, maintaining, processing and/or transmitting electronic personal health information. Concern for the privacy and security of that information prompted the United States Congress to enact legislation requiring those technology companies to implement a wide variety of procedures to ensure the privacy and security of such information. The legislation also provides for civil and criminal penalties for those who fail to comply.

The federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") imposes upon health care providers, health care clearing houses and health care plans ("Covered Entities") legal obligations to comply with certain procedures and requirements designed to ensure the privacy and security of personal health information. Two years ago, Congress extended HIPAA's privacy and security rules to "business associates" of those Covered Entities. The new legislation is called the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

Who Must Comply?

Business associates of Covered Entities must comply with the HITECH Act. "Business associates" includes any person or company that (i) assists a Covered Entity in performing a function or activity involving the use or disclosure of individually identifiable health information; or (ii) provides consulting, management, administrative or other services to or for a Covered Entity where the provision of services involves the disclosure of individually identifiable health information.

Most Covered Entities will treat any information technology or Internet service company that possesses individually identifiable health information in the course of providing its products or services as a "business associate" and will therefore require compliance with the HITECH Act as a prerequisite to doing business with the company.

What are the Compliance Requirements of the HITECH Act?

The HITECH Act is complex, and a complete listing of the HITECH Act's requirements is beyond the scope of this publication. However, some of its requirements include the following:

The HITECH Act requires business associates to implement certain administrative, physical and technical safeguards in order to protect the privacy and security of the personal health information with which they deal. Those safeguards include the following:

(i) Administrative Safeguards

- Business associates must adopt and implement written policies and procedures to prevent,

For more information about the HITECH Act and its compliance requirements, please contact Daniel Appelman at dappelman@mh-llp.com or at 650-331-7014.

detect, contain and correct security violations. These policies and procedures must include risk assessment, security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, sanctions against employees who fail to comply with the security policies and procedures of the covered entity, procedures to regularly review records of system activity such as audit logs, access reports and security incident tracking systems.

- Business associates must identify a security official who is responsible for the development and implementation of the policies and procedures mentioned above.

- Business associates must implement policies and procedures to limit the access of their workforces to electronic personal health information.

- Business associates must implement security awareness and training programs for all members of their workforces (including management).

- Business associates must institute and document security incidence response and reporting procedures that are reasonably designed to identify and respond to suspected or known security incidents, to mitigate the harmful effects of such incidents and to document the security incidents and their outcomes.

- Business associates must establish policies and procedures for responding to breaches of security or other occurrences that damage systems that contain electronic personal health information. These policies and procedures should include a data backup plan, a disaster recovery plan and a plan for an emergency mode of operation in the event of damage to their systems.

- Covered entities may not give business associates access to electronic personal health information unless the covered entity obtains satisfactory assurances that the business associate has adequate policies and procedures to safeguard the information. The documentation of these assurances must be in a written contract.

(ii) Physical Safeguards

- Business associates must implement policies and procedures to limit physical access to their electronic information systems and the facilities in which they are housed.

- Business associates must implement policies and procedures designed to maintain the security and proper functioning of workstations that contain or can access electronic personal health information.

- Business associates must implement policies and procedures to address the destruction or other final disposition of electronic personal health information in their possession.

(iii) Technical Safeguards

- Business associates must implement technical policies and procedures to limit access to systems that contain electronic personal health information.

- Each user having access to electronic personal health information through the business associate must have a unique name or number for identifying and tracking user identity.

- Business associates must adopt procedures for obtaining access to electronic personal health information during an emergency.

- The services offered by business associates must include mechanisms that terminate electronic sessions after a predetermined period of inactivity.

- Business associates must implement mechanisms to encrypt and decrypt electronic personal health information.

- Business associates must implement electronic mechanisms to corroborate that electronic personal health information has not been altered or destroyed in an unauthorized manner.

- Business associates must implement procedures to verify that a person seeking access to electronic personal health information is the one claimed.

- Business associates must implement technical security measures to guard against unauthorized access to electronic personal health information that is being transmitted over an electronic communications network.

The HITECH Act requires business associates to develop and maintain a set of written policies and procedures that address the administrative, physical and technical safeguards just described and that provide guidance to the company's employees as they handle personal health information (including electronic information) on behalf of their Covered Entity clients.

The HITECH Act requires business associates to enter into written contracts with their Covered Entity clients in which they promise to comply with the requirements of the HITECH Act.

The HITECH ACT requires business associates to notify their Covered Entity clients when they become aware of any breach in the security of personal health information. The notification must be made without unreasonable delay, and it must identify the individuals whose personal health information has been compromised.

The HITECH ACT prohibits business associates from marketing or selling personal health information.

What are the Consequences of Not Complying with the HITECH Act?

Both civil and criminal penalties are available for violations of the HITECH Act.

Enforcement by Secretary of Health and Human Services

The Secretary of Health and Human Services ("HHS") may impose penalties ranging from $100 per violation to $1,500,000. The penalties are arranged in tiers and increase depending on whether the violation was unintentional or due to willful neglect. "Willful neglect" is determined on a case-by-case basis. Business associates who have simply ignored the compliance requirements or who have not undertaken a good faith effort to comply will likely be found to be in willful neglect of their legal obligations.

Enforcement by State Attorneys General

The state Attorneys General may also bring civil or criminal action against those who violate the HITECH Act. Civil penalties range from $100 to $25,000 plus a recovery of attorneys fees. Criminal penalties range from $50,000 and/or a year in prison to $250,000 and ten years in prison depending on the nature of the violation.

Current Developments Regarding the HITECH Act

The Office of Civil Rights ("OCR") within the Department of Health and Human Services is developing final rules for extending HIPAA's privacy and security compliance requirements to business associates of Covered Entities. The final rules will be released by the end of 2011. In the meantime, the OCR has announced interim rules on enforcement and breach notification that are being enforced.

We will publish subsequent bulletins when the final privacy and security compliance rules are issued.

Implications for Technology Companies Offering Services to Covered Entities

Concern for the privacy and security of personally identfiable information is increasing as that information is converted to electronic form and becomes available online. In no area is the concern more intense than in the area of health care and the medical and financial records of patients. As health care providers reach out to technology companies to provide electronic services, the need for those companies to undertake measures to safeguard an limit access to personal health information becomes increasingly evident.

HIPAA has not been rigorously enforced. In enacting the HITECH Act, Congress sent Covered Entities and their business associates a clear message that lax enforcement would no longer be tolerated. The extension of significant compliance obligations to those who provide services to health care providers, and the increased penalties for violating those obligations, present a challenge to technology companies that they will ignore at their peril. These companies will need to devote considerable time and resources to complying with the HITECH Act's requirements. Many of those requirements will be subject to future regulatory and judicial interpretation. It will be important for our technology company clients to keep up to date with the implementation of the HITECH Act as the final rules are announced by the OCR and as HHS and the state Attorneys General begin their enforcement activities.