Health Law Bulletin

provided by:

MITCHELL • BLACKSTOCK

Mitchell • Blackstock • Barnes • Wagoner • Ivers • Sneddon • PLLC

YOUR HIPAA POLICIES MUST BE REVISED TO MEET HITECH RULES

The recently enacted economic stimulus bill contains new requirements for all those who handle Protected Health Information ("PHI"). The Health Information Technology for Economic and Clinical Health Act ("the HITECH Act") creates significant new responsibilities, risks and penalties for health care providers and their business associates who have access to PHI.

The HITECH Act imposes new notice requirements in connection with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The requirements apply to both the Covered Entity and the Business Associate. If unsecured PHI is improperly released, a notification must be sent to the individual and to the federal Department of Health and Human Services "without unreasonable delay" and in no case later than 60 days after the discovery of the breach by either a Covered Entity or a Business Associate. If the breach involves 500 or more persons, then notice must be provided to the news media in the area. "Unsecured" PHI is defined as PHI that is not secured through the use of technologies or methodologies that render it "unusable, unreadable or indecipherable to unauthorized individuals." This change in the law makes it even more crucial that health care providers and their business associates maintain up-to-date electronic safeguards for their PHI, such as encryption.

The new law mandates periodic audits of Covered Entities and Business Associates to check for compliance with HIPAA and HITECH. Such audits likely will include a review of policies and procedures, security of PHI, and analysis of the unauthorized disclosures list.

Liability for unauthorized release of unsecured PHI and penalties for violations have been drastically changed. Business associates are made directly liable for violations of HIPAA or of HITECH, so business associates must follow the same HIPAA Security Rules as a Covered Entity. State Attorneys General may sue under the HITECH Act to obtain an injunction or monetary damages for violations of HIPAA. The amount of federal civil monetary penalties for violations has been increased up to a maximum of $1.5 million per calendar year. Individuals who have been harmed by improper disclosure of their PHI may be able to receive a percentage of the imposed civil monetary penalty.

Different provisions of the HITECH Act have different implementation dates, and regulatory guidance has not yet been issued. Health care providers and their business associates should begin preparing now for compliance with these mandatory rules. Among the steps that providers will need to take are: (1) revising business associate contracts and communicating with business associates regarding their new obligations; (2) conferring with computer systems staff regarding whether PHI is fully secured under the standards of HITECH; (3) ensuring that current policies and procedures are in place and that staff is fully trained; and (4) establishing documentation requirements for monitoring and periodic reviews, notice of breach and mandatory reporting. If you need assistance in revising your HIPAA policies, preparing for an audit, or revising your HIPAA Business Associate agreements, you may want to consult an attorney.

--May 4, 2009