HITECH: New Security and Privacy Requirements

Employment, Labor & Benefits Practice Group
Foster Swift Employment, Labor & Benefits Quarterly
Spring 2010

PRACTICE AREAS

Employee Benefits
Employment Law
Health Care
Labor Relations
Technology Law

On February 17, 2010, most of the Health Information Technology for Economic and Clinical Health Act ("HITECH") became binding on the health care industry. The HITECH Act was passed as part of the American Recovery and Reinvestment Act to promote utilization of electronic health records ("EHR"). Along with providing monetary incentives for the utilization of EHR, the HITECH Act imposes an extensive regulatory scheme to protect EHR.

SECURITY AND PRIVACY REQUIREMENTS FOR BUSINESS ASSOCIATES

Specifically, HITECH applies portions of the Health Insurance and Portability Act ("HIPAA") to entities ("Business Associates") that receive protected health information ("PHI") when providing services to Covered Entities. Previously, only health care providers, health care clearinghouses, and health plans ("Covered Entities") were subject to HIPAA's regulations and civil and criminal penalties. But as of February 17, 2010, Business Associates will be required to comply with the HIPAA security regulations as well as additional HITECH Act privacy and security requirements. The security requirements fall into three specific categories: administrative, physical, and technical safeguards.

Administrative safeguards include:

- implementing security management processes (including risk analysis and management, applying sanctions for violations, and information system activity reviews)
- assigning security responsibility
- implementing workforce security (including authorization processes, workforce clearance procedure, and terminating access procedures)
- establishing information access management
- implementing security awareness training programs for the entire workforce
- implementing security procedures, monitoring, and updates
- establishing a contingency plan

- doing periodic evaluations of the policies and procedures
- establishing business associate contracts with covered entities

Physical Safeguards include establishing:

- policies and procedures to limit physical access to information systems (including contingency and facility security plans, access control and validation of access to the facility and equipment, and maintenance records)
- workstation use and security
- device and media controls

Technical safeguards include implementing:

- access controls (such as unique user identification and emergency access procedures)
- audit controls
- integrity controls
- person/entity authentication
- transmission security

Additionally, the HITECH Act requires a Business Associate to notify the Covered Entity following the discovery of an unauthorized acquisition, access, use or disclosure of PHI. The HITECH Act also requires a Business Associate to take action if a Covered Entity consistently fails to comply with the Business Associate Agreement. Specifically, the Business Associate must take reasonable steps to end the violation. Otherwise, the Business Associate must terminate the contract or report the problem.

IMPACT ON COVERED ENTITIES

Covered Entities as well as Business Associates should change (or if applicable, adopt) their current Business Associate Agreements to ensure compliance with the HITECH Act. Covered Entities should also ensure that all of their Business Associate relationships are indeed covered by Business Associate Agreements as the civil penalties for "reasonable cause" and "willful neglect" have increased to potential fines of $100,000 and $1.5 million respectively.