Recent Changes to HIPAA – the HITECH Act

Introduction

Among tax cuts and credits, more bailout fund requirements, and restrictions on executive pay packages, the American Recovery and Reinvestment Act of 2009 (ARRA) also includes a section that expands the reach of the Health Insurance Portability and Accountability Act (HIPAA) and introduces the first federally mandated data breach notification requirement.

Title XIII of ARRA, also known as the Health Information Technology for Economic and Clinical Health Act (HITECH Act), reserves $22 billion to "advance the use of health information technology" - in large part so the U.S. will be able to move to e-health records by President Obama's 2014 deadline. It also expands the reach of HIPAA data privacy and security requirements to include the "business associates" of those entities (health care providers, pharmacies, and the like) that are subject to HIPAA. Business associates are companies like accounting firms, billing agencies, law firms or others that provide services to the entities covered under HIPAA.

Under the HITECH Act, those companies are now directly subject to HIPAA security and privacy requirements, as well as to the same civil and criminal penalties that hospitals, pharmacies and other HIPAA-covered entities face for violations. Before HITECH came into force, business associates that failed to properly protect patient information were liable to the covered entities via their service contracts, but they did not face governmental penalties.

Stronger Enforcement & Stiffer Penalties

The most significant changes in the HITECH Act are those that strengthen HIPAA enforcement measures. In particular, subsection 13410(c), requires civil penalties that are collected under the HITECH Act to be funneled back into the Department of Health and Human Services' Office of Civil Rights enforcement budget. Moreover, monetary penalties are mandatory for violations involving "willful neglect" as of Feb. 17, 2011. In addition, the fine for a HIPAA complaint will be increased from $25,000 to $1,500,000. The HITECH Act also provides for the Department of Justice to pursue criminal penalties for a violation that rises to the level of criminal activity. However, in the event that DOJ declines to act on a violation, the HITECH Act allows OCR to pursue civil penalties for that same violation.

The expanded opportunity for state attorneys general to get involved in enforcement under the HITECH Act will create more complexity for those subject to HIPAA - especially those who do business in more than one state. The HITECH Act's data breach notification requirements for protected health information add another level of complexity. Currently 44 states require organizations to notify affected individuals, legal authorities, and the media in the event of a data breach related to personal information. However,

only two of these states (California and Arkansas) require such notification for breach of health data and the federal government has never addressed the issue - until now.

Increased Notification Requirements

The HITECH Act requires HIPAA-covered entities to notify the Secretary of Health and Human Services and affected individuals when their protected information has been compromised. Notice must be given to the individuals whose data is affected "without unreasonable delay," and no later than 60 days after the breach occurs. Similarly, business associates that experience a breach are required to notify the covered entities with which they have contracted, and the covered entities will then notify the affected individuals. If the breach involves 500 people or more, the covered entity will also be required to notify major media outlets.

The fact that Congress chose to limit the requirements to health information complicates matters further for companies that operate in several states. They are already subject to the various state data breach notification requirements, which can be different and at times inconsistent. And those will still apply to information other than in the health arena. So those companies can't simply come up with a form letter that will work for every breach.

Implications for IT Asset Retirement

The Department of Health and Human Services issued guidance related to safe harbors for healthcare providers to avoid mandatory data breach notification. The guidance states that if computer hard drives are disposed after sanitization meeting National Institute for Standards and Testing (NIST) specification SP 800-88, data breach notification will not be required. It also states that that destroying paper media in a manner that it “cannot be read or otherwise cannot be reconstructed” provides that same safe harbor.

It is important to note that none of this is actually a requirement of HIPAA or HITECH—it is simply advice regarding safe harbors for avoiding possible data breach notification events.

Conclusion: Get Prepared

Privacy analysts universally predict that the modifications raise the stakes substantially for all involved and expect much more focus on compliance, contingency planning, and business associate selection. All agree that the best strategy is to be prepared. Covered entities and business associates alike should, at a minimum, review their current security programs (including IT asset retirement procedures) to ensure that they are in compliance. Covered entities should notify their business associates of the changes in ARRA, and begin working on a plan to revise their business associate contracts to reflect the changes. HIPAA.com also provides a "to-do list" to help business associates prepare. The list includes such tasks as appointing a security official and developing written policies and procedures that include both physical safeguards (locking computers) and technical safeguards (encrypting e-mail). Training employees on how to protect electronic health information is also important.