

# “What keeps you up at night?”

Saul Ewing Health Law  
Practice Group:

George W. Bodenger  
Chair

## Economic stimulus act toughens HIPAA privacy and security requirements

By Scott D. Patterson

On February 17, 2009, President Obama signed into law the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), as part of the American Recovery and Reinvestment Act of 2009 (“Recovery Act”).

The HITECH Act is primarily designed to encourage investment in health information technology (HIT). However, the expansion of HIT and the contemplated development of national infrastructures for the exchange of health information will dramatically increase the volume of patient information in circulation. With this in mind, Subtitle D (Privacy) of the HITECH Act includes multiple sections “improving” privacy and security requirements imposed by the Health Insurance Portability and Accountability Act of 1996 and related regulations (HIPAA). These “improvements” significantly expand parties’ HIPAA obligations. They will force both “covered entities” (healthcare providers, clearinghouses, and health plans) and “business associates” (such as service providers, third-party administrators, and health information exchanges) to revisit and update their HIPAA compliance programs and related business associate agreements. The Recovery Act is framed as an economic stimulus bill, but this portion of the legislation will initially act as a stimulus for accelerated compliance activity.

### EXPANSION OF BUSINESS ASSOCIATE OBLIGATIONS

The HITECH Act subjects business associates to privacy and security obligations that now apply only to covered entities, including requirements for implementation of administrative, physical, and technical data safeguards, establishment of compliance policies and procedures, and documentation of compliance and disclosures. Business associates will also become subject to civil and criminal penalties equivalent to those faced by covered entities. Health Information Exchanges (HIEs), Regional Health Information Organizations (RHIOs), e-Prescribing Gateways, and other entities will become expressly subject to business associate obligations.

## “What keeps you up at night?”

### NOTIFICATION OF DATA AND SECURITY BREACHES

In another dramatic expansion of HIPAA requirements, the HITECH Act will require covered entities and business associates to provide specified notifications when a breach of “unsecured” protected health information (PHI) occurs. Fortunately for those charged with managing HIPAA compliance programs, this notification requirement will not become effective until 30 days after publication of “interim final” HHS regulations, which HHS is mandated to issue within 180 days (mid-August 2009). Initially, unsecured PHI is defined as PHI “that is not secured by a technology standard that renders [PHI] unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by [ANSI]” (e.g., HL7 or ASC X12). The final standard will be set by a guidance document to be developed this year by HHS, specifying qualifying technologies and methodologies.

A covered entity such as a healthcare provider or health plan will be required to notify each individual whose unsecured PHI has been compromised. Notice must be given “without unreasonable delay” and in any event no more than 60 days after any employee, officer, or agent (other than the one committing the breach) knows or “should reasonably have known” that a breach has occurred. A covered entity is also required to submit an annual log to HHS documenting all breaches that have occurred during the year, and must notify HHS “immediately” of any breach affecting more than 500 individuals’ PHI. Similarly, if a business associate discovers a breach, it must give timely notice to the covered entity, which will then be obligated to provide appropriate notice to affected individuals and HHS. The contents and methods of notification are prescribed in detail, and include a posting on the HHS website and notice to “prominent media outlets” for breaches involving more than 500 individuals’ information. A “breach” is broadly defined (with some exceptions) as any “unauthorized acquisition, access, use, or disclosure of [PHI] which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” These definitions and requirements will be refined in the future interim final regulations.

Similar notice requirements are imposed on “vendors of personal health records [PHRs]” following the discovery of a breach of secu-

urity of “unsecured PHR identifiable health information that is in a [PHR] maintained or offered by such vendor,” and on otherwise non-covered entities who offer products and services through PHR vendors’ websites, if the breach occurred through their products or services. A “breach of security” is simply acquisition of an individual’s PHR identifiable health information without his or her authorization. In this setting, notice must also be given to the Federal Trade Commission, and a failure to give required notices will be considered an “unfair or deceptive act or practice” subject to FTC enforcement action. Like HHS, the FTC is required to issue interim final regulations by August 2009, and these enforcement provisions will apply to security breaches discovered 30 or more days after the regulations are published.

### MISCELLANEOUS CHANGES

Covered entities must confine their PHI disclosures to “limited data sets” or the “minimum necessary” to accomplish its intended purpose, and HHS is directed to issue future guidance on what constitutes the “minimum necessary”. Individuals will have access to their PHI held in an electronic record, with limits on the fees that can be charged for that access. Individuals are also given the right to demand an “accounting” from covered entities of all disclosures of their EHRs made for treatment, payment, and healthcare operations purposes, beginning as of January 2011 (or January 2014 in the case of PHI already in existence as of January 2009). The HITECH Act also prohibits entities from receiving remuneration for PHI if the patient has not specifically given a valid authorization for the provider’s receipt of remuneration, and it imposes significant marketing and fundraising restrictions effective a year from now (February 2010).

### ENFORCEMENT

The HITECH Act also strengthens enforcement and increases penalties. State attorneys general are empowered for the first time to bring civil enforcement actions on behalf of state residents threatened or adversely affected by HIPAA violations, and to collect attorneys’ fees if they are successful. Persons harmed by an unauthorized disclosure may eventually be entitled to receive a percentage of civil money penalties collected by the federal government. HHS audits of covered entities and business associates are also prescribed. The enforcement and penalty provisions are effective immediately.

While it will take some time for the full impact of this legislation to be assessed, both covered entities and business associates will need to start planning now for the changes it prescribes. If you have questions about these requirements or any other provisions of the HITECH Act, please feel free to contact any of the Saul Ewing attorneys listed below.

Scott D. Patterson at [spatterson@saul.com](mailto:spatterson@saul.com) or 610.251.5089

Bruce D. Armon at [barmon@saul.com](mailto:barmon@saul.com) or 215.972.7985

Laura L. Katz at [lkatz@saul.com](mailto:lkatz@saul.com) or 410.332.8804

George W. Bodenger at [gbodenger@saul.com](mailto:gbodenger@saul.com) or 215.972.1955

---

This Alert was prepared by Scott D. Patterson, a Partner and Chair of Saul Ewing's Healthcare Technology Contracting Practice Group. Scott can be reached at [spatterson@saul.com](mailto:spatterson@saul.com) or 610.251.5089. This publication has been prepared by the Health Law Practice Group for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute "Attorney Advertising."

© 2009 Saul Ewing LLP, a Delaware Limited Liability Partnership.  
ALL RIGHTS RESERVED.