Paul Hastings
StayCurrent
A CLIENT ALERT FROM PAUL HASTINGS
March 2009

Stronger Protections for Health Information are Part of the Fiscal Stimulus

BY BEHNAM DAYANIM, ERIC KELLER AND KELLY DEMARCHIS

A key part of the fiscal stimulus package (the "Act"), signed by President Obama into law on February 17, 2009, included sweeping changes to the health information privacy and security provisions promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[1] Many of these new protections will take effect February 17, 2010 (one year after enactment of the Act); however, some have their effective dates delayed until the Department of Health and Human Services ("HHS") provides specific guidance. The Act calls for guidance in several areas, so increased rulemaking activity should be expected from HHS in the coming months.

Among other things, the Act imposes many of its security standards directly on business associates, enacts new notification requirements for a breach of unsecured protected health information ("PHI"), expands disclosure obligations for covered entities and rights for individuals who are the subject of the PHI, and increases penalties and grants enforcement authority beyond HHS to include states' attorneys general. These new changes are discussed further below.

Business Associates are Subject to Direct Regulation

The Act imposes some of HIPAA's privacy standards and many of HIPAA's security standards directly on "business associates." "Business associate" generally is defined as an entity that provided services such as claims processing, data analysis, and billing to covered entities. Until now, business associates were exempt from direct regulation although they were subject to certain requirements by contract.

Now, business associates are directly subject to the technical, physical, and administrative provisions in the HIPAA security standards just as are other covered entities. This change will require business associates to pursue a variety of responses, including undertaking a risk analysis, appointing a compliance officer and developing written policies and procedures to govern the security of electronic PHI, among other items. In addition, the Act requires business associates to use and disclose PHI only in accordance with the HIPAA privacy standards that apply to business associate contracts. Consequently, a business associate that breaches a business associate contract violates the HIPAA privacy standards. Under the Act, business associates now also will be subject to civil and criminal penalties for violations of HIPAA's privacy and security standards.

New Breach Notification Rules

One of the most significant changes included in the Act is a new patient notification requirement.

Currently, most states and several federal financial regulatory agencies require various forms of notice (either to individuals or agencies) in the event of unauthorized access to or misappropriation of personal information. However, HIPAA did not previously require covered entities to report those types of breaches.

The Act adds a notification requirement that applies to all covered entities and business associates. They must notify individuals of a breach of their "unsecured PHI" within 60 days of discovery of the breach. (HHS is to promulgate technical guidelines for securing PHI within 60 days after the enactment of the Act.) Covered entities are deemed to have knowledge of a breach under the Act if they "should reasonably have known" of the breach. Notification must be written and sent by first-class mail to the individual's last known address, or can be electronic mail if the individual previously specified a preference for electronic notice. If there is insufficient or out-of-date contact information, covered entities may substitute conspicuous posting on its webpage or notice in major print or broadcast media. Substitute notice must include a toll-free phone number that an individual can call to verify if his or her PHI was affected.

Breaches that affect more than 500 individuals also must be reported to HHS, which will publicize the breach on the HHS website. For breaches that affect fewer than 500 people, the covered entities may keep a log to be submitted annually to HHS.

Expanded Individual Rights and Disclosure Obligations

The Act grants individuals certain additional rights. Individuals may request an electronic copy of their PHI if the information is stored electronically and the copy must be provided at cost. Individuals may restrict disclosures of their PHI to a health plan, if the purpose of the disclosure is not related to treatment and the individual paid the full cost of the services that generated the PHI. Covered entities must honor this request. Individuals also may request an accounting of disclosures of their electronic PHI if the disclosures were made for treatment, payment, and health care operations purposes.

The Act directs HHS to issue guidance by August 17, 2010, on what constitutes the "minimum necessary" for purposes of satisfying HIPAA's requirement to limit uses, disclosures, and requests for PHI to the "minimum necessary" to achieve the intended purpose of the use, disclosure, or request. Until that guidance is issued, the Act provides that covered entities must use, disclose, or request only a "limited data set" in order to meet this requirement, to the extent practicable. A limited data set is a subset of PHI that is stripped of the majority of identifiers, including name, contact information, medical record number, social security number, IP address, URL, and full-face photographic images.

The Act also places conditions on marketing communications sent by covered entities, which require the patient's written consent prior to sending the communication, with some exceptions. HIPAA previously defined "marketing communication" as a communication about a product or service that encouraged the recipient of the communication to purchase or use the product or service, unless the communication was deemed to be for treatment or health care operations purposes. The Act now prohibits using PHI in connection with treatment or health care operations purposes if the covered entity receives direct or indirect payment from a third party in connection with the communication. It also prohibits the sale of PHI, whether electronic or paper, without the patient's authorization, with some exceptions. HIPAA did not previously directly prohibit such sales.

Increased Penalties and Expanded Enforcement

The Act significantly increases civil monetary penalties and introduces a tiered penalty structure. Penalties, which were $100 per

violation (and capped at $25,000 for multiple violations), have risen to $1,000 per violation if due to "reasonable cause and not to willful neglect" (capped at $100,000 per calendar year), $10,000 for each violation due to "willful neglect" that is corrected (capped at $250,000 per calendar year), and $50,000 for each violation due to "willful neglect" that is not corrected (capped at $1,500,000 per calendar year).

The Act also clarifies that criminal penalties may apply to an individual or employee of a covered entity that obtains PHI without authorization.

Although individuals do not have a private right of action under HIPAA, state attorneys general are now authorized to file suit on behalf of their residents.

In addition to enforcement, HHS is now required to conduct periodic audits of covered entities and business associates to verify compliance with HIPAA's privacy and security requirements. HHS is also required to investigate formally all complaints.

✧ ✧ ✧

Behnam Dayanim, Eric Keller, and Kelly DeMarchis practice in the Paul Hastings Washington, D.C. office. The Paul Hastings Privacy and Information Security Practice advises clients on all areas of personal data privacy and security regulation, conducts compliance assessments of privacy and security practices, represents clients in regulatory investigations and litigation, and advocates at a public policy level in these areas.

For more information about the new HIPAA rules, please contact:

Washington D.C.

Behnam Dayanim
202-551-1737
bdayanim@paulhastings.com

Eric Keller
202-551-1770
erickeller@paulhastings.com

Kelly DeMarchis
202-551-1828
kellydemarchis@paulhastings.com

1 The complete citation for the Stimulus Plan is the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, H.R. 1, 111th Cong. (2009). The sections reforming HIPAA can be found at §§13400-13424 of the Act.