

Stimulus Law Includes Major Changes to HIPAA Privacy and Security Rules

The American Recovery and Reinvestment Act of 2009 (the Act)¹, signed into law by President Obama on February 17, 2009, contains funding for health information technology (HIT) programs that are designed to encourage the adoption of electronic health records (EHRs) by health care providers. It is hoped that EHRs, which are electronic records used by health care clinicians and providers, will create efficient transfers of medical information and perhaps facilitate better medical treatment. Along with the HIT programs, the law enacts a number of significant changes to the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. Most of these changes take effect one year after enactment, but breach notification requirements will take effect later this year.

KEY HIPAA CHANGES

This section summarizes the key HIPAA changes affecting group health plans.

Breach Notification Required by Fall 2009

The Act contains two separate provisions addressing breach notification: one applicable to HIPAA covered entities and business associates, and the other applicable to vendors of personal health records (PHR)² and other entities linked to PHRs. This *Bulletin* discusses only the covered entity requirement, but the PHR breach notification requirement has similar rules.

¹ When the law, Public Law No. 111-5, is available online, it will be accessible from the following page of the Government Printing Office Web site: <http://www.gpoaccess.gov/plaws/111publ.html>

² Under the Act, a PHR is an electronic record of identifiable health information managed, shared, and controlled by or primarily for an individual. This is distinct from an electronic health record (EHR), which contains health-related information about an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.

This notice requirement applies to breaches discovered 30 days after the publication of interim final regulations, which are required to be published not later than 180 days after enactment. If those regulations are published on time, this breach notification requirement will apply to breaches discovered after mid September 2009.

For the first time, group health plans will be required to provide notice to affected individuals when there is a breach involving “unsecured protected health information.” The Act defines this term as protected health information (PHI) that is not secured through the use of a technology or methodology specified by the Secretary of Health and Human Services (HHS). The Act requires the Secretary to issue, within 60 days of enactment, guidance on these specific technologies and methodologies.

Notice must be provided without unreasonable delay, and in no case later than 60 calendar days after the breach is discovered, to each affected individual and to the Secretary of the HHS. (Notice must be provided to the HHS “immediately” if the breach affected 500 or more individuals). In some cases, the media must also be notified.

The notice must include a description of what happened, the types of PHI involved, the steps that individuals should take to protect themselves, the steps the covered entity is taking to investigate and mitigate harm, and contact information for follow-up questions.

If a HIPAA business associate is responsible for the breach, the business associate must notify the covered entity of the breach, listing each individual whose PHI was, or is reasonably believed to have been, accessed, acquired or disclosed.

New Approach to Business Associates

Group health plans typically rely on HIPAA business associates to perform a variety of functions involving the use or disclosure of PHI. Business associates include third party administrators (TPAs), pharmacy benefit managers (PBMs), health benefits administration system vendors, attorneys, actuaries and consultants. Plans are already required to enter into a HIPAA business associate agreement (BAA) with

each business associate, spelling out the business associate's privacy- and security-related obligations.

Effective one year after enactment, HIPAA business associates will have a direct statutory obligation to comply with most of the HIPAA security rule and to comply with the privacy-related obligations contained in their BAAs. They will also be subject to direct civil and criminal penalties.

Minimum Necessary Standard

The privacy rule's minimum necessary standard governs nearly all uses, disclosures, and requests for PHI. The Act requires the Secretary to issue guidance on the minimum necessary standard within 18 months of enactment. However, beginning February 17, 2010, and continuing until that guidance is issued, covered entities will be deemed to be in compliance with the minimum necessary standard if, to the extent practicable, they use, disclose, or request a "limited data set" — which, under the privacy rule, means a data set stripped of nearly all identifiers. Group health plans generally cannot use limited data sets for health plan operations.

Other Key Changes

The stimulus law makes the following other changes to the HIPAA privacy rule, all of which are effective February 17, 2010 except for the changes in the first bullet, which are effective immediately (*i.e.*, for violations after February 17, 2009).³

- Significant increases in civil monetary penalties (topping out at \$1.5 million per year per standard violated for the most egregious violations) and enforcement by state attorneys general,
- Expansion of enforcement to include actions against employees of covered entities and business associates and required periodic audits of covered entities and business associates,
- Requires covered entities to agree to a request by a plan participant or beneficiary to restrict disclosure of PHI if the disclosure is to a health plan and the treating health care provider has been paid in full out of pocket,
- New restrictions on marketing communications where the covered entity receives direct or indirect remuneration for making the communication, and
- New fundraising restrictions that require clear and conspicuous notice of the right to opt out of receiving further communications.

³ A few other changes not discussed here (*e.g.*, ban on sale of PHI) have a longer compliance timeframe.

ACTION STEPS FOR PLAN SPONSORS

Plan sponsors need to be prepared to provide breach notification, as early as this fall, and also need to:

- Update their HIPAA policies and procedures to reflect the changes made by the Act, and provide training on these changes to members of their workforce,
- Review existing BAAs to determine if contract amendments are necessary, and incorporate the Act's new requirements into new BAAs, as appropriate,
- Consider whether the HIPAA privacy notice needs to be revised in light of changes to the individual right to request a restriction on the use and disclosure of PHI, and
- Review liability insurance contracts to determine whether any changes are necessary to assure coverage for potential HIPAA violations.



As with all issues involving the interpretation or application of laws and regulations, plan sponsors should rely on their attorneys for authoritative advice on the interpretation and application of the American Recovery and Reinvestment Act of 2009. Sibson Consulting can be retained to work with plan sponsors and their attorneys on HIPAA compliance, as modified by the Act.

SIBSON CONSULTING A DIVISION OF SEGAL

ATLANTA	678.306.3100
BOSTON	617.424.7300
CALGARY	403.692.2264
CHICAGO	312.984.8500
CLEVELAND	216.687.4400
DENVER	303.714.9900
HARTFORD	860.678.3000
HOUSTON	713.664.4654
LOS ANGELES	310.231.1700
MINNEAPOLIS	952.857.2480
MONTREAL	514.989.3735
NEW ORLEANS	504.483.0744
NEW YORK	212.251.5000
PHILADELPHIA	215.854.4017
PHOENIX	602.381.4000
PRINCETON	609.520.2700
RALEIGH	919.233.1220
SAN FRANCISCO	415.263.8200
TORONTO	416.969.3960
WASHINGTON	202.833.6400

www.sibson.com