

Practice Areas
Health Care

Good Company

HIPAA Gets a Stimulus: Major Changes to Privacy and Security Rules

Tuesday, June 30, 2009

The American Recovery and Reinvestment Act of 2009, informally known as the “Stimulus Bill”, has brought dramatic changes to the HIPAA Privacy and Security Rules. Covered entities, such as health care providers, employer sponsored health plans and insurers, and business associates are significantly affected, and even vendors of personal health records will feel the impact.

New Obligations to Notify Individuals and HHS of Breaches - Effective 2009

For the first time, HIPAA covered entities will have to give specific notification to individuals if the entity discovers their unsecured protected health information (PHI) was improperly used or disclosed. Covered entities must also notify the US Department of Health and Human Services (HHS) of all breaches. (Remember that state law requirements regarding security breaches also continue to apply, including New Hampshire RSA 359-C:19-21.)

Within 60 days of discovery of a breach, a covered entity must give notice via first class mail to the affected person’s last known address, or by email if specified as a preference by that person. Included, among other things, must be (i) a description of what happened, (ii) the date of the breach (if known), (iii) the date of discovery, (iv) a description of the information involved in the breach, (v) the steps the person should take to protect him/herself, (vi) a description of the covered entity’s investigation and its efforts to mitigate the harm created by the breach, (vii) an outline of what the entity is doing to protect against further breaches, and (viii) contact information at the entity for any questions. If current contact information for the affected individuals is unavailable, the covered entity may be required to post notice of the breach on its own website or in newspapers or other broadcast media. For large breaches (affecting more than 500 people), both HHS and “prominent media outlets” must also be notified. Annual reports to HHS of smaller breaches are also required.

All business associates must report breaches to their covered entities, including the identity of each affected person.

The breach notification requirements apply only to “unsecured” PHI, which is information that is not secured through a technology or methodology that HHS has determined renders it “unusable, unreadable or indecipherable” to unauthorized persons. HHS issued guidance on April 17, 2009 stating that PHI secured through encryption or destruction according to specified standards would not be considered unsecured PHI.



**SHEEHAN
PHINNEY
BASS +
GREEN PA**
the business law firm

Covered entities and business associates have an incentive to use these technologies or methodologies (and follow the guidance) because then there will be no “unsecured PHI” and none of the breach notification provisions will apply. Covered entities and business associates should still review state law breach notification provisions to see if they apply, however.

Regulations to implement the above changes must be issued by August 17, 2009 and the requirements will be effective for breaches discovered on or after 30 days after issuance.

Expansion of Privacy and Security Rules to Business Associates - Effective February 2010

The most consequential change is that business associates will now have to comply directly with many of HIPAA’s Security and Privacy Rules, instead of being made to comply contractually by covered entities. Specifically, business associates must comply with administrative, physical and technical safeguards and requirements for policies, procedures and documentation in the Security Rules, with which covered entities are already required to comply. This means, for example, that business associates will have to implement physical safeguards for all workstations that access electronic PHI, restrict access to authorized users, implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI, assign unique names and/or numbers for identifying and tracking user identities, implement a security awareness and training program, and conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by them. Failure to comply means that HHS (and now state attorneys general) may bring actions and impose fines directly against business associates. Compliance will place a significant burden on business associates, and is likely to increase the cost and legal risks of being a business associate to a covered entity.

All existing business associate agreements must be amended and updated to ensure they include the new obligations under the Stimulus Bill.

Enhanced Enforcement, New Tools and Compensation to Individuals for Breaches - Effective 2009 into 2012

Effective immediately, civil money penalties for violations of HIPAA have been significantly increased. Penalties now range from \$100 to \$50,000 per violation, with a maximum in any one year ranging from \$25,000 to \$1.5 million.

State attorneys general are also now empowered to bring civil HIPAA enforcement actions directly against covered entities and business associates. In addition, the new law requires HHS to investigate complaints, impose penalties for willful neglect and conduct periodic audits of both covered entities and business associates to ensure they are in compliance with the rules. Audits were possible but infrequent under the old rules due to a lack of staffing and funding. However, some monetary penalties and settlements will be transferred to the HHS Office of Civil Rights to be used for the purposes of enforcing HIPAA so better funding will now be available. All of these things combined are likely to result in far more investigations of complaints and much greater enforcement activity than ever before.

HHS must also establish an education initiative by February 2010 to enhance public transparency about the uses of PHI, including educating the public about the potential uses of PHI, the effects of such uses and the rights of individuals. By 2012, HHS must have a program in place to distribute portions of collected penalties to people whose PHI was improperly used or disclosed, which will create a significant financial incentive for individuals to report suspected HIPAA violations.

Mandated Compliance with Requests for Restrictions on PHI - Effective February 2010

Under current the HIPAA Privacy Rules, a person can ask a covered entity to restrict certain uses or disclosures

of PHI, but the covered entity does not have to agree to the request. However, starting in February 2010, if a person requests a restriction on a disclosure to a health plan for payment or health care operations purposes and the PHI pertains only to services for which the covered entity has been paid in full by the person on a self-pay basis, then the covered entity must agree and comply.

Electronic Medical Records: Access/Accounting - Effective February 2010; 2011-2014

Starting in February 2010, if a covered entity uses or maintains an electronic medical record, an individual has the right to receive, or have sent to a third party, a copy of the PHI maintained in his/her electronic record in an electronic format. Any fee charged to that person may not exceed the labor costs actually incurred in responding to the request.

Under the present rules, individuals have the right to receive an accounting of disclosures from a covered entity, except for certain disclosures including those made for purposes of treatment, payment or health care operations. Under the new changes, however, if a covered entity maintains PHI in an electronic health record, the covered entity will have to track and include *all* disclosures for purposes of treatment, payment and health care operations in an accounting to a person. HHS is to provide guidance as to what will have to be collected about treatment, payment and health care operations disclosures. If a covered entity acquired an electronic health record as of January 1, 2009, then any disclosures made through that record must be tracked and reported in the accounting to an individual starting January 1, 2014. For any electronic health records acquired by the covered entity after January 1, 2009, such disclosures must be tracked and reported starting January 1, 2011. HHS is permitted to delay both of these effective dates up to two years. It seems likely that there will be considerable lobbying for HHS to do just that.

Covered entities have the option of giving an accounting of all disclosures that both it and its business associates make, or just giving an accounting of its own disclosures along with a list of all business associates and contact information so the individuals can request the accounting directly from the business associates. The latter creates a much greater burden on business associates.

Prohibition on Sale of EHR or PHI - Effective 2010-2011

Covered entities and business associates will be prohibited under the new law from receiving any payment in exchange for any PHI, unless the person who is the subject of the PHI gives specific written authorization allowing them to do so. There are certain limited exceptions, including for purposes of treatment or sale, transfer, merger or consolidation of covered entities, and research. Regulations to implement this provision must be issued by August 2010 and will apply to exchanges that occur within 6 months after the regulations are issued.

Marketing and Fundraising Communications - Effective February 2010

The changes tightened restrictions on use of PHI for marketing and fundraising purposes by clarifying that communications which are "marketing" (and require patient authorization) under the current HIPAA Privacy Rules may not be treated as "health care operations" (which do not require authorization). Further, communications that fall within the current exceptions to the marketing definition are not allowed if the covered entity is paid to make the communication unless certain requirements are met. Finally, all fundraising communications that are considered health care operations must provide, in a clear and conspicuous manner, an opportunity for the recipient to elect not to receive any further such communications, similar to the current requirements for fundraising communications that do not fall into health care operations. This appears directed at covered entities who have been treating their fundraising as part of health care operations to avoid the current opt-out requirement.

Vendors of Personal Health Records Now Covered - Effective 2009



**SHEEHAN
PHINNEY
BASS +
GREEN PA**
the business law firm

The Stimulus Bill also extends to vendors of personal health records, requiring that they and other non-covered entities and non-business associate entities that interact with personal health records comply with certain breach notification requirements. The FTC is required to issue regulations no later than August 2009 which will apply to breaches of security on or after 30 days from the date of issuance. The FTC issued proposed rules on April 16, 2009. Once enacted, violations of these rules will be treated as unfair and deceptive acts or practices violating the Federal Trade Commission Act, subject to the same fines and penalties.

Watch for New Regulations

As noted above, the Stimulus Bill requires HHS to issue a number of new HIPAA regulations, covering such things as (1) implementation of requirements for notification of breaches, (2) description of the information that must be collected when tracking disclosures of electronic medical records for purposes of an accounting, (3) implementation of the prohibition on the sale of information from electronic medical records, (4) implementation of mandatory HHS investigations and penalties for violations due to willful neglect, and (5) establishment of a methodology for distributing a percentage of collected penalties and settlements to persons harmed by HIPAA violations.

Be sure to monitor the ongoing HIPAA rulemaking, and the FTC rules if you are a vendor of personal health records (note that it is possible to be a business associate in certain instances and a direct vendor in other situations), so you will be prepared to comply. You should also begin assessing what changes will be required in your policies and procedures as a covered entity or business associate to comply with the new rules, determining what changes need to be made to your business associate agreements and training your workforce in the new requirements.

This article is intended to serve as a summary of the issues outlined herein. While it may include some general guidance, it is not intended as, nor is it a substitute for, legal advice. Your receipt of Good Company or any of its individual articles does not create an attorney-client relationship between you and Sheehan Phinney Bass + Green or the Sheehan Phinney Capitol Group. The opinions expressed in Good Company are those of the authors of the specific articles.