CHANGES TO HIPAA UNDER THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

Client Advisories

03.19.2009

BY: WILLIAM P. ISELE, ESQ

On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act of 2009, otherwise known as the Stimulus Act or ARRA (hereinafter, "the Act"). In addition to appropriating billions of dollars for economic recovery, the Act makes some important changes to the Privacy Rules promulgated under the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA.

1. Extension of HIPAA's Privacy Rules to Business Associates

Under the HIPAA Privacy Rules, covered entities (i.e., health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form) must enter into written agreements with their business associates before disclosing protected health information ("PHI") to the business associate. Such agreements have extended the Privacy Rules to business associates in a limited fashion.

Section 13401 of the Act extends the Privacy Rules to business associates, essentially resulting in the conversion of business associates into covered entities. Business associates must now comply with the existing Privacy Rules, as well as new security provisions set forth in the Act. Business associates will now be directly responsible to ensure that their uses and disclosures of PHI comply with the Privacy Rules.

The Act also requires that these new requirements be incorporated into the parties' written agreements. Thus, covered entities will have to revise their existing business associate agreements to comply with the Act.

Section 13401(b) and section 13404(c) should remove any doubt that business associates who violate the HIPAA Privacy Rules will be subject to the same civil and criminal penalties as covered entities. Until now, it was generally agreed that there would be no civil and criminal penalties for violations of HIPAA by business associates.

Section 13408 of the Act expands the category of "business associate" to include organizations that contract with covered entities for the purpose of exchanging PHI, such as a Health Information Exchange Organization, Regional Health Information Organization or E-prescribing Gateway. Such organizations must enter into business associate agreements with the covered entities before any protected health information may be exchanged.

2. Notification of Breaches of Information

In the event of a breach of an individual's "unsecured protected health information," Section 13402 of the Act requires covered entities to notify each individual whose PHI has been breached, within 60 days of discovery of the breach. In the event of a breach of "unsecured protected health information" under the control of a business associate, the business associate will be required to notify the covered entity of the breach, and identify each individual whose PHI has been breached, also within 60 days. If the breach of "unsecured protected health information" involves more than 500 individuals, covered entities also must notify prominent media outlets serving the State or jurisdiction, and the Secretary of the U.S. Department of Health and Human Services ("DHHS"). If a breach involves fewer than 500 individuals, the covered entity need not notify the Secretary immediately, but may maintain a log of such breaches and submit it annually to DHHS. DHHS will also post on its website a list of covered entities involved in breaches of "unsecured protected health information" of more than 500 individuals. Sub-sections 13402 (e) and (f) of the Act contain detailed requirements for the method of notice and the information that must be included in each notice.

3. Restrictions on Disclosures of Protected Health Information

Until now, HIPAA gave individuals a right to request that a covered entity restrict certain disclosures of protected health information ("PHI"), but covered entities were not required to honor the request. Under Section 13405(a) of the Act, covered entities are now required to comply with an individual's request to restrict disclosures of PHI to a health plan, if the disclosure is for purposes of payment or health care operations, but not for purposes of carrying out treatment, and the PHI pertains solely to a health care item or service for which the individual paid out-of-pocket in full.

4. **Expansion of Minimum Necessary Standard**

Section 13405(b) of the Act requires covered entities to limit the use, disclosure or request of PHI to a "limited data set," if practicable, or the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The Act requires the Secretary of DHSS to issue guidance on what constitutes "minimum necessary." Sub-section 13405(b)(2) clarifies that the entity disclosing the PHI, as opposed to the requester of information, is the one who makes the minimum necessary determination.
Again, the Privacy Rule's exceptions to the minimum necessary rule, such as disclosures to or by a health care provider for the treatment of an individual, will continue to apply.

5. Accounting of Disclosures of PHI in EHRs

Section 13405(c)(1)(B) of the Act grants individuals a right to receive an accounting, for up to three years prior, of disclosures of PHI made for treatment, payment and health care operations purposes, if the disclosures are through an electronic health record ("EHR"). The Secretary of DHSS is required to issue regulations on what information must be collected about each disclosure.

Curiously, for covered entities currently using EHR, the new accounting requirement would apply to disclosures made on or after January 1, 2014. For covered entities yet to acquire EHR, the requirement would apply to disclosures made on or after January 1, 2011, or the date it acquires EHR, whichever is later. Section 13405(c)(4).

6. Sales of PHI; Revised Definition of Health Care Operations & Marketing

Section 13405(d) of the Act adds a provision prohibiting a covered entity or business associate from receiving direct or indirect remuneration in exchange for PHI, subject to seven specific exceptions.

Section 13406 tightens the rules regarding communications about products or services that a covered entity or business associate markets to patients. The Act eliminates from the definition of "health care operations" communications made by a covered entity or business associate about health care related products or services, if the covered entity or business associate making the communication receives "direct or indirect remuneration" for making the communication. Communications are limited to drugs or biologics currently being prescribed for the recipient of the communication, where any payment received by the covered entity is reasonable in amount. A covered entity may not market a health care related product or service without first obtaining the recipient's authorization.

Finally, the Act prohibits covered entities from using PHI for fundraising purposes unless the written fundraising communication provides the recipient with an opportunity to opt out of future fundraising communications.

The Act requires the Secretary to revise the definition of "health care operations" to eliminate those activities that can reasonably and efficiently be conducted with de-identified information or that should require authorization for the use or disclosure of PHI.

7. Increased Enforcement and Penalties

Section 13410 of the Act makes the following significant revisions to the enforcement and penalties provisions under HIPAA:

- Requires that any civil monetary penalties collected be transferred to the Office of Civil Rights of the HHS to be used for enforcing the Privacy Rules.
- Requires the Secretary to make recommendations for giving a percentage of any civil monetary penalty to the individuals harmed, and regulations for such distribution.
- Establishes a tiered system of civil monetary penalties. The first tier is for violations where the person did not know, or in the exercise of reasonable diligence, would not have known it was a violation. The second tier is for violations due to "reasonable cause." The third tier is for violations due to willful neglect, where

the violation is corrected. The fourth tier is for violations due to willful neglect that is not corrected. For each tier, penalty amounts are established per violation, and cumulative maximum amounts per year.

- Authorizes State Attorneys General to bring civil actions in federal district court against anyone who violates the Privacy Rules for injunctive relief or damages on behalf of individuals harmed. Costs and attorneys fees may be awarded to the State.
- Requires the Secretary to perform periodic audits to ensure that covered entities and business associates are in compliance with Privacy Rules.

The foregoing summary describes the changes to HIPAA in general terms. HIPAA-covered entities are strongly encouraged to review their policies and procedures carefully with counsel in light of the details of the Act, and revise them to assure that they are in conformity with the changes in Federal Law.

For more information, please contact a member of Archer's Health Care Law Practice Group in Haddonfield at (856) 795-2121, Princeton at (609) 580-3700 or Philadelphia at (215) 963-3300.

Related People

William P. Isele

Of Counsel

wisele@archerlaw.com

609.580.3780

Related Services

- Healthcare