Shipman & Goodwin LLP

HIPAA Alert

March 2009

STIMULUS PACKAGE SIGNIFICANTLY EXPANDS HIPAA REQUIREMENTS

The economic stimulus package, officially named the American Recovery and Reinvestment Act of 2009 (the "Act"), which President Obama signed into law on February 17th, includes extensive changes to the privacy and security rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Act expands the HIPAA privacy and security rules and includes other changes that will require action on the part of covered entities and business associates.

I. Expanded Scope of HIPAA Applicable to Business Associates

HIPAA has traditionally regulated only certain covered entities and not business associates directly. The Act expands HIPAA's applicability and now directly applies HIPAA's security and privacy rules to all business associates – independent contractors of covered entities who use or disclose protected health information ("PHI") in connection with their services on behalf of the covered entity.[1] Business associates must now implement all of the administrative, physical and technical safeguards required by HIPAA for a covered entity and have policies, procedures and documentation to establish its compliance. Moreover, a violation of the privacy and security rules will subject the business associate to the same civil and criminal penalties applicable to covered entities. This significantly increases the obligations of a business associate beyond what was previously required. Thus, covered entities must revise their business associate agreements to ensure that their business associates comply with HIPAA in accordance with the Act.

---

[1] In addition to expanding the responsibilities and penalties applicable to business associates, the Act also expands the definition of business associate to include organizations that provide data transmission of PHI to covered entities. Such entities include, among others, Health Information Exchange Organizations, Regional Health Information Organizations and E-prescribing Gateways.

II. Notification of Breach

The Act requires certain notifications by both covered entities and business associates if there is a "breach" (i.e. the unauthorized acquisition, access, use or disclosure of unsecured PHI that compromises the security or privacy of such information).

Notice to the patient. A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI must, upon breach, notify each individual whose PHI has been, or reasonably believed to have been, accessed, acquired or disclosed as a result of such breach. Up until now, HIPAA has not required that patients be notified of a breach.

Notice to the covered entity. In the case of a business associate, the business associate must notify the covered entity of a breach by the business associate.

Notice to the Media and the Secretary. In breaches involving the PHI of at least 500 individuals, the covered entity must notify "prominent media outlets." In addition, the covered entity must notify the Secretary of the Department of Health and Human Services (HHS) who in turn will post notice of such breach on the HHS website.

A breach will be treated as discovered on the first day the breach becomes known, or reasonably should have been known. The Act provides detailed information on how to give notice and the content of the notice.

III. Disclosures

Restrictions Requested by Patient. A covered entity must now abide by a request for restriction from an individual if the disclosure is to a health plan for purposes of carrying out payment or health care operations (not treatment) and the PHI relates to services for which the health care provider has been paid out of pocket in full. Up until now, covered entities were not required to agree to this restriction.

Accounting of Disclosures for Electronic Records. Covered entities and business associates that use or maintain electronic health records must provide an accounting of disclosures upon request from an individual, including disclosures for treatment, payment and health care operations for a period of three years from the date of the disclosure. A covered entity that receives such a request may either provide the accounting of disclosures by the entity and business associates or provide the individual with contact information to allow the individual to contact the business associates directly. If contacted, a business associate must provide the accounting. This change is not applicable to paper medical records.

The new accounting requirements are effective between 2011 and 2014. The date by which a covered entity must be prepared to meet this expanded accounting obligation depends on the date when the covered entity acquired an electronic health record. A covered entity that acquired an electronic health record as of January 1, 2009 must account for disclosures of

PHI made by the covered entity on and after January 1, 2014. Covered entities that acquire an electronic health record after January 1, 2009 must account for disclosures of PHI made by the covered entity on and after the later of January 1, 2011 or the date that the covered entity acquired the electronic health record.

Access in Electronic Format. In connection with an individual's right to access his or her medical record under HIPAA, the Act gives individuals the right to receive an electronic copy of their PHI, if it is maintained in an electronic health record. The covered entity may charge a fee for such access in order to cover its labor costs for providing the electronic copy if permitted by State law.

IV. Sale of PHI

New Marketing Permitted. HIPAA defines marketing as a communication about a product or service intended to induce the recipient to buy or use the product or service advertised. The use of PHI for marketing generally requires the authorization of the individual. There were three exceptions to marketing when the covered entity could use PHI without authorization, including describing a health-related product or service (or payment therefor), treatment of the individual or case management and care coordination. Before the Act, it appeared as if the covered entity could be paid to provide PHI for the three permitted marketing activities. The Act now provides that the covered entity can only be paid if:

- The communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and the payment is deemed reasonable; and
- The communication is made by a covered entity and that entity has received a valid authorization from the recipient; or
- The communication may be made by a business associate on behalf of the covered entity and is consistent with the relevant written contract between the parties.

Sale of PHI. The Act provides that a covered entity may not sell or charge for PHI except in certain specified circumstances, such as to recoup the costs of preparing and transmitting data for public health or research activities, or to provide an individual with a copy of his or her PHI.

V. Personal Health Records

The Act mandates new requirements for vendors that provide or maintain unsecured personal health records. A personal health record is an electronic record of individually identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or for the individual (e.g. Google Health). The Act requires that the vendor notify both the affected individuals and the Federal Trade Commission ("FTC") of any breaches. The FTC is required to respond to the breach as an unfair trade practice.

Additionally, the Act imposes requirements on vendors' third-party service providers to notify the vendor of a breach and include the identification of each individual whose unsecured information has been, or is reasonably believed to have been, acquired, accessed or disclosed.

VI. Increased Enforcement

The Act contains several provisions that will likely lead to the increased frequency and severity of enforcement actions and penalties.

Enforcement. The Act strengthens enforcement of HIPAA provisions by expanding the roles of the HHS Office of Civil Rights ("OCR"), the attorneys general of each state and affected individuals. OCR is now required to investigate complaints involving willful neglect and required to audit covered entities and business associates for violations of HIPAA's privacy and security standards. Penalties obtained from enforcement are to be transferred to OCR to fund future enforcement. Attorneys general of each state are given new authority to file civil actions or injunctions in federal court to enforce HIPAA. Attorneys general of each state may also recover attorneys' fees and costs associated with such actions. The Act does not change the traditional rule that HIPAA does not provide for a private right of action, but does provide that individuals who are harmed by a HIPAA violation may receive a percentage of any penalty collected for such violation.

Penalties. Effective immediately, the law increases the civil penalties that may be imposed, up to $1,500,000 depending on the type of violation (i.e. uncorrected violations due to willful neglect).

VII. Action Items

While different parts of the Act have different deadlines and some of the deadlines are delayed until after HHS issues final regulations, covered entities and business associates should start taking steps to comply.

Business Associate Agreements. All covered entities should amend their HIPAA business associate agreements with all business associates, now including organizations that provide data transmission services. Changes will include modified breach provisions, the application of privacy and security provisions and new rules for accounting for disclosures.

Business Associates. Business associates must now comply with HIPAA's security and privacy standards and must take action to ensure such compliance. Business associates should consider how they will comply with HIPAA, including:

- appointing a HIPAA compliance officer;
- developing written HIPAA policies and procedures; and
- employee trainings.

Effective Dates. While the Act generally becomes effective February 17, 2010, there are requirements of the Act that become effective immediately or at later dates.

Unanswered Questions. Congress left a few unanswered questions in the Act that may be answered in future regulations to be issued by HHS, including the following:

- ***Technology Guidance***. Many covered entities and business associates struggle with the question of what technology is sufficient to protect electronic PHI. The Act requires HHS to issue annually updated guidance specifying the technologies and methods that will be considered sufficient to render electronic PHI secure.
- ***Minimum Necessary Standard***. The Act requires covered entities to limit the use, disclosure or request of PHI to the minimum necessary to fulfill the intended purpose of the use, disclosure or request. HHS has eighteen (18) months to issue guidance on what constitutes minimum necessary.
- ***Reports***. The Act requires various governmental agencies to report on certain issues involving HIPAA or the Act, including information regarding complaints, the application of privacy and security rules to noncovered entities, how to best de-identify PHI, best practices for treatment disclosures and the use and disclosure of psychotherapy notes. This appears to indicate that there may be additional changes to HIPAA in the future to address these issues.
- ***Education***. HHS must designate an individual in each region to offer guidance and education to covered entities, business associates and individuals on their rights and responsibilities under HIPAA. OCR must develop and maintain a national education initiative to increase transparency regarding the uses of PHI.

Questions or Assistance?

If you have any further questions regarding the HIPAA rules, please feel free to contact either Joan Feldman or David Mack.

Joan Feldman
(860) 251-5104
jfeldman@goodwin.com

David Mack
(860) 251-5058
dmack@goodwin.com

This communication is being circulated to Shipman & Goodwin LLP clients and friends. The contents are intended for informational purposes only and are not intended and should not be construed as legal advice. This may be deemed advertising under certain state laws. Prior results do not guarantee a similar outcome. © 2008 Shipman & Goodwin LLP.

SHIPMAN & GOODWIN LLP
COUNSELORS AT LAW