

February 2009

HIPAA Alert

Stimulus Bill Dramatically Modifies HIPAA Rules — Business Associates and Covered Entities Must Address New Requirements

The American Recovery and Reinvestment Act (the “Act”; also informally known as the “Stimulus Bill”) was signed into law by President Obama on February 17, 2009. The Act contains surprising modifications to HIPAA's Privacy and Security Rules. These changes will likely require every business associate agreement to be modified. The Act also, for the first time, requires business associates to comply directly with many of HIPAA's rules and subjects business associates to HIPAA's civil and criminal penalties. The Act increases the penalties for various HIPAA violations and dramatically expands other remedial actions (such as increasing federal government audits; granting attorneys fees in some HIPAA lawsuits; and allowing a method for individuals to recover penalties under HIPAA). The changes are significant to all covered entities, but are most challenging for business associates, who now face a host of new requirements.

Security Rules Apply Directly to Business Associates. For the first time, business associates must comply directly with many of HIPAA's Security Rules. This will require every business associate to take several actions, including appointing a security official, developing written policies and procedures, and training its workforce on how to protect electronic protected health information (“EPHI”). These provisions go well beyond the previous requirements for business associates, where business associates only had to comply with the written business associate agreement.

Business associates also will need to follow HIPAA's Security Rules relating to physical safeguards (such as locking computers that contain EPHI), technical safeguards (such as encrypting emails) and the requirement to adopt written policies and procedures. Failing to do so will – for the first time – subject a business associate to civil monetary penalties and criminal penalties for each notification (and, as discussed below, the civil monetary penalties are now increased).

New Security Breach Rules. Under current law, the breach of the privacy or security of protected health information (“PHI”) often does not require significant action by a covered entity or business associate. This changes under the Act. Now, a covered entity or business associate that has a specified security breach will be required to notify each individual affected by the security breach. This can involve written notification by mail or, if specified by preference by the individual, email. If the covered entity or business associate lacks current contact information, it may be required to post notice of the breach on its website or in newspapers or other broadcast media (e.g., television). For certain large breaches (involving more than 500 residents in a particular area) a “prominent media outlet” must be notified of the breach. The U.S. Department of Health and Human Services (“HHS”) also must be contacted, and HHS is to establish a website listing these breaches. There is an exception for certain unintentional breaches.



WILL THE ACT REQUIRE CHANGES TO MY HIPAA FORMS? These new changes almost certainly will require changes to a health plan's current HIPAA forms. For business associates without any current HIPAA forms, the business associate must create the forms for the first time. The Act is likely to require several changes to existing HIPAA forms. For example, the breach provisions specify the type of information that must be collected and provided to individuals, HHS and media outlets. This information includes a brief description of what happened, including the date of the breach, the date of the discovery of the breach along with the steps individuals should take to protect themselves from potential harm resulting from the breach. A covered entity also must disclose what it is doing to investigate the breach, to mitigate losses and to protect against any further breaches. In order to gather all this data, a covered entity must modify its policies and procedures and related forms to ensure it has a process in place to gather the data, then communicate it in a manner required by the new law.

HHS Guidance and Appropriate Technologies and Methodologies. Currently there is considerable confusion about what technologies and methodologies covered entities and business associates should use to protect EPHI. For example, must all email be encrypted? If so, what encryption software programs are sufficient? For the first time, HHS is required to issue, and annually update, guidance specifying the technologies and methodologies that will render EPHI secure. Covered entities and business associates are likely to welcome any additional guidance in this area.

Certain Privacy Rules Apply Directly to Business Associates. The Act states that business associates must comply directly with certain HIPAA Privacy Rules, primarily the requirement to have and follow a business associate agreement. The scope of this change is unclear. It could mean that every entity must determine whether it is a business associate with respect to a covered entity. If so, the business associate may be required to enter into a business associate agreement with the covered entity. Previously, it was a covered entity's responsibility to identify all its business associates (a business associate did not need to identify whether it actually was a business associate).

Changes to Restriction Request Rules. Currently, HIPAA allows an individual to request that certain PHI not be used by a covered entity or business associate. This is known as a restriction request. Current law generally allows the covered entity to decline all such requests. Now, under the Act, a covered entity must comply with the restriction request in certain circumstances (if the disclosure is to a health plan for purposes of carrying out payment or health care operations (not treatment) and the PHI pertains solely to a health care item or service for which the health care provider has been paid in full).

New Rules Regarding Electronic Health Records. The Act creates a new term, "electronic health record", which is an electronic record of health-related information on an individual that is "created, gathered, managed, and consulted by authorized health care clinicians and staff." It is not clear whether this term applies only to such health records when they are held by an authorized health care clinician or the related staff. When such a health record is transferred to a health plan, employer or business associate, it is not clear whether the Act's requirements will continue to apply.

The Act imposes significantly more disclosure accounting requirements relating to electronic health records. Currently, a covered entity or business associate need not track its disclosures of PHI if the PHI is used to carry out treatment, payment or healthcare operations. This is very helpful, because most disclosures of PHI fall into one of these exceptions, so the disclosure need not be tracked. Now, under the Act, if the disclosure of an electronic health record is for treatment, payment or healthcare operations,



the covered entity (and a business associate) must maintain an accounting of such a disclosure. There is a delayed effective date for this provision, such that it will apply sometime between January 1, 2011 and January 1, 2014.

Prohibition on Sale of Electronic Health Records or PHI. The Act states that a covered entity or business associate cannot directly or indirectly receive remuneration in exchange for any PHI unless it first obtains a valid authorization from the individual whose PHI is being disclosed.

Access to Electronic Health Records. The Act states that if a covered entity uses or maintains an electronic health record with respect to PHI, an individual shall have the right to obtain from the covered entity a copy of such information in "electronic format". It is not clear what the term "electronic format" means, and whether an individual can request a particular electronic format (or if the individual can only receive the information in an electronic format selected by the covered entity).

Changes to Definition of Healthcare Operations. Currently, many health plans and business associates may send out communications to plan participants to encourage the participants to use a product or service. This will still likely be possible, but the rules have become more restrictive and these types of communications must be examined more thoroughly to ensure that they remain proper.

Other Vendors of Personal Health Records Now Covered. The new rules go beyond regulating business associates and covered entities. The new rules also cover any "vendor" of "personal health records." The new rules impose security standards on such vendors and require the Federal Trade Commission (not HHS) to help enforce these new rules. The new rules appear to apply to certain vendors (such as Microsoft and Google) that have begun collecting health records even though the vendor is not a covered entity or business associate.

New Business Associate Contracts Required for Certain Entities. Certain organizations that transmit PHI on behalf of a covered entity or business associate must have a business associate contract (or similar contract) in place with the covered entity (or business associate).

Significant Overhaul of Civil Monetary Penalties. The civil monetary penalties are significantly increased. Currently, the amount of the penalty is generally \$100 for each violation. This \$100 amount (and its related cap of \$25,000 for multiple violations) increases to \$1,000 per violation for a violation due to "reasonable cause and not to willful neglect" (with a maximum penalty of \$100,000); \$10,000 for each violation that was due to willful neglect and is corrected (subject to a \$250,000 maximum penalty); and \$50,000 for each violation if the violation is not corrected properly (subject to a maximum penalty of \$1,500,000 during a calendar year). These changes are immediately effective (i.e., they are in effect today) and represent a dramatic increase in the penalties under HIPAA.

In addition, state attorney generals can now bring a HIPAA enforcement action against a covered entity or business associate that violates these rules. Further, the state attorney general can obtain attorney's fees under such an action (although the attorney's fees are discretionary and not mandatory).

HHS – the main enforcer of HIPAA – now is required to conduct "periodic audits" to ensure that both business associates and covered entities are compliant with these new rules. Audits were possible under the old regulations. However, audits tended to be fairly rare, perhaps due to a lack of funding at HHS. Now, some monetary penalties or settlements collected by HHS are transferred to HHS's Office of Civil Rights to be used for purposes of enforcing HIPAA. This appears to solve the funding issue that HHS had apparently experienced. Thus, clients can expect to see increased HIPAA audits and enforcement.



Individuals Can Receive Compensation for Breaches. The Act requires HHS to establish a regulation, within the next three years, providing that individuals affected by a HIPAA violation will be able to receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense. Previously, it was difficult, if not impossible, for individuals to receive such amounts. This change alone may cause an increased interest in enforcement activity, as individuals (and their lawyers) will now have a financial incentive to bring HIPAA complaints and accusations of HIPAA violations.

Effective Date. The general effective date for the Act is February 17, 2010. However, many of the provisions have varying effective dates and others have an effective date that is unclear. Business associates and covered entities should examine each provision carefully.

Model Documents to Assist in Compliance. In March, 2009 we will make available our updated model documents for health plans and business associates. Please contact one of the attorneys below for more information about these documents or about any of the items discussed in this alert.

For more information, please contact one of the authors of this alert or your Michael Best attorney.

This client alert is one of a series designed to provide summaries of the American Recovery and Reinvestment Act of 2009 ("The Act") and information and guidance regarding opportunities and relief made available through The Act. All of The Act client alerts are available on Michael Best's [Stimulus and Economic Recovery Team publications page](#). For additional information on this topic, please feel free to contact one of the authors of this alert or your Michael Best attorney.

If you are interested in learning about other provisions included in the Act, the Michael Best [Stimulus and Economic Recovery Team](#) is prepared to assist you in understanding the implications and in developing and implementing a strategy to secure the benefits of this unprecedented legislation. Specifically, we will assist you to identify opportunities, prepare appropriate proposals and make targeted contacts to secure funds. We will also work with you to ensure that your applications are tailored to meet your needs and that your funded projects proceed in compliance with award requirements and applicable laws.

