SMITH ANDERSON

Client Alert

March 2009

HITECH Act Expands Scope and Enforcement of HIPAA

Signed into law on February 17, 2009, the American Recovery and Reinvestment Act of 2009 (the "ARRA") includes the most expansive changes to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") since the issuance of the final privacy and security regulations in 2002 and 2003, respectively. Specifically, Title XIII, Subtitle D of the ARRA, known as the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act" or the "Act"), contains provisions that significantly expand the scope and force of the privacy and security regulations under HIPAA. These changes are part of the Obama administration's goal to facilitate the electronic exchange of health information between all healthcare providers.

With these changes, a wide range of businesses may find it necessary to revisit their HIPAA compliance efforts. Many of the Act's provisions are set to become effective February 17, 2010; however, certain provisions may become effective as early as six months from the date of enactment, and certain enforcement and penalty provisions became effective *upon the date of enactment* of the Act. The changes under the Act affect covered entities and their business associates (business associates commonly include technology vendors and consultants that access protected health information while providing services to covered entities), as well as vendors of personal health records. Notably, the Act makes several of the HIPAA privacy and security regulations directly applicable to business associates, subjecting them to the same civil and criminal penalties as covered entities. The Act also includes breach notification provisions, places limits on the sale of protected health information, and expands the enforcement mechanisms and penalties for violations of HIPAA. Some of the more significant provisions of the Act are set forth below.

EXPANSION OF THE HIPAA PRIVACY RULE AND THE HIPAA SECURITY RULE

Currently, only covered entities, and not business associates, are directly subject to the requirements of HIPAA. HIPAA applies to business associates indirectly, by way of the business associate's contractual obligations to the covered entity. The Act changes this by making certain provisions of the HIPAA Privacy Rule and the full spectrum of requirements under the HIPAA Security Rule directly applicable to business associates. Some of these changes are described below.

HIPAA Privacy Rule

The HIPAA Privacy Rule requires covered entities to enter into business associate agreements with their business associates and enumerates required provisions related to the use and disclosure of protected health information ("PHI"). The business associate's compliance with the terms of a business associate agreement, however, is governed by the agreement, and not directly by HIPAA.

The Act changes this by making a business associate's compliance with the terms of a business associate agreement a direct requirement of HIPAA. Specifically, the Act states that when a business associate obtains or creates PHI pursuant to a business associate agreement, it may use and disclose such PHI only if it complies with

each requirement of 45 C.F.R. § 164.504(e) (the HIPAA provision that outlines the requirements for a valid business associate agreement).

The Act also increases the oversight role that business associates have over covered entities with whom they contract. Specifically, the Act requires business associates to: (a) take reasonable steps to cure a breach of a business associate agreement, or (b) terminate the agreement if it knows of a pattern of activity or practice by a covered entity that violates the agreement. If terminating the agreement is not feasible, the business associate may be required to report the covered entity to the Secretary of the Department of Health and Human Services (the "Secretary").

HIPAA Security Rule

Currently, with respect to the HIPAA Security Rule, business associates must contractually agree to use "appropriate safeguards" to prevent the unauthorized use or disclosure of PHI accessed on behalf of a covered entity. This represents only a limited portion of the HIPAA Security Rule requirements. The Act, however, subjects business associates to the full HIPAA Security Rule. Business associates will be required to implement the administrative, physical, and technical safeguards, as well as the organizational requirements, policies, procedures, and documentation requirements of the HIPAA Security Rule.

What Do These Changes Mean?

Business associates will be required to enter into modified business associate agreements to address these changes. Perhaps even more significant, however, is the need for business associates to establish and broaden existing privacy and security policies and procedures to address these new requirements.

Examples of such measures include implementing security awareness and training programs for workforce members, creating and implementing policies and procedures governing the use and protection of PHI, designating appropriate privacy and security officials, and conducting periodic privacy risk assessments.

Non-compliance with these changes may constitute a *direct violation* of HIPAA, leaving business associates open to potential contractual liability as well as HIPAA enforcement actions and resulting civil and criminal penalties. The Act sets these provisions to become effective February 17, 2010. The scope of these changes, however, means that affected parties should begin to revisit privacy compliance efforts now.

NEW DATA BREACH NOTIFICATION PROVISIONS

Currently, under HIPAA, a covered entity does not have an affirmative obligation to notify an individual of a data breach involving the unauthorized disclosure of PHI about the individual. A covered entity is obligated merely to track such disclosures and provide an accounting of those disclosures in response to the individual's request. Business associates, on the other hand, are required only to report such disclosures to the covered entity. Where there has been a specified breach of "unsecured" PHI, the Act provides new notification provisions applicable to covered entities, vendors of personal health records, and related entities, and more rigorous reporting requirements applicable to business associates.

Covered entities will be required to notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of a breach that is discovered by the covered entity. This provision applies to a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI. Specified forms of notification, including certain content described under the Act, must be made to the individual without unreasonable delay, but in no event later than 60 calendar days after discovery of the breach.

Business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI must notify the covered entity of a data breach discovered by the business associate. The notice must include, among other things, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed as a result of the breach.

The Act also requires vendors of personal health records, regardless of whether they qualify as covered entities or business associates, to notify the Federal Trade Commission and each affected individual of any such data breaches.

The Secretary is required to issue regulations implementing these breach notification provisions within 180 days of the date of enactment (by August 16, 2009), and such provisions will apply to data breaches discovered 30 or more days from the publication of such regulations.

LIMITATIONS ON SALE OF PHI

The Act includes restrictions limiting the sale of PHI by covered entities and business associates. Absent a specific exception, the Act generally prohibits covered entities and business associates from receiving remuneration in exchange for PHI *unless* the covered entity obtains a HIPAA-compliant authorization from the individual. The authorization must also expressly state whether the PHI may be further exchanged for remuneration by the entity receiving the PHI.

The Act sets out six specific exceptions where this restriction will not apply. The restriction will not apply in cases where the purpose of the exchange is:

- For public health activities;
- For research activities where the price charged reflects the cost of preparation and transmittal of the data;
- For treatment of the individual;
- For the specific health care operation involving the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that, following such activity, will become a covered entity, and due diligence related to such activity;
- For remuneration that is provided by a covered entity to a business associate for activities involving the exchange of PHI; and
- To provide an individual with a copy of the individual's PHI.

The Secretary is required to issue regulations to carry out this provision no later than 18 months after enactment (by August 17, 2010). The limitations on the sale of PHI will apply to exchanges of PHI beginning six months after such regulations are implemented.

EXPANDED ENFORCEMENT RIGHTS

Effective *upon enactment* of the Act, state attorneys general were authorized to bring civil actions against individuals who violate HIPAA. An attorney general bringing a civil action under HIPAA must give the Department of Health and Human Services the opportunity to intervene in the action. The Act also requires the Secretary to formally investigate complaints where a preliminary investigation indicates a potential violation of HIPAA due to willful neglect, but this change is not set to take effect until February 17, 2011.

GREATER PENALTIES FOR HIPAA VIOLATIONS

Effective *upon enactment* of the Act, the civil penalties for HIPAA violations were increased. The Act provides tiered increases in the amounts of such penalties, as follows:

- If the person did not know of the violation, a penalty of at least $100 per violation, not to exceed $50,000 for each violation.
- If the violation was due to reasonable cause and not to willful neglect, a penalty of at least $1,000 per violation, not to exceed $50,000 for each violation.
- If the violation was due to willful neglect, a penalty of at least $10,000 per violation, not to exceed $50,000 for each violation; provided, however, that if the violation is not corrected, the penalty shall be no less than $50,000 per violation.

OTHER NOTABLE CHANGES

In addition, the Act contains new limitations on marketing activities involving PHI by covered entities and business associates and expands certain rights of individuals to receive an accounting of disclosures from a covered entity and to limit disclosures of PHI about the individual.

Affected parties will need to monitor issuance of applicable regulations and any guidance that clarifies or changes these new provisions in order to address them appropriately within their organizations. If you have questions about these or other privacy matters, please contact one of the Smith Anderson lawyers listed below or the Smith Anderson lawyer with whom you work.

Bo Bobbitt
919.821.6612
bbobbitt@smithlaw.com

Alicia Gilleskie
919.821.6741
agilleskie@smithlaw.com

Frederick Zufelt
919.821.6727
fzufelt@smithlaw.com

SMITH, ANDERSON, BLOUNT, DORSETT, MITCHELL & JERNIGAN, L.L.P.

Offices:
2500 Wachovia Capitol Center
Raleigh, North Carolina 27601
Mailing Address:
Post Office Box 2611
Raleigh, North Carolina 27602
Telephone: 919-821-1220
Facsimile: 919-821-6800
Email: Info@smithlaw.com