LEWIS AND ROCA LLP LAWYERS

CLIENT Alert

September 2009

Stimulus Legislation Expands HIPAA Regulations

By Gregory Y. Harris

The "Stimulus" legislation enacted by Congress shortly after President Obama became President included significant changes to HIPAA that directly affect businesses which handle patient protected health information (PHI), particularly those that have entered into business associate agreements with covered entities. These changes, contained in the HITECH Act, amend HIPAA and affect the privacy and security rules adopted by the federal government under HIPAA.

This client alert outlines some of these important changes. The HITECH Act makes significant portions of HIPAA specifically applicable directly to business associates. Previously, HIPAA applied only to covered entities, such as insurance companies and providers. The rules established that covered entities had an obligation to police the business activities of their "business associates." However, neither the original statutory language of HIPAA nor the rules adopted by the federal government following the enactment of HIPAA imposed mandates directly upon business associates. This all changed with the enactment of the HITECH Act.

The changes enacted as part of the HITECH Act extend both to the HIPAA Privacy Rule and the HIPAA Security Rule. Because these changes may apply equally to covered entities, their business associates and business associates of business associates, this refers to all three collectively as "entities"—unless the context requires otherwise.

Implementation of the Security Rule

The HIPAA Security Rule—until the recent law change applied only to covered entities—has now been specifically made applicable to business associates. This Rule consists of five core elements, documentation of which must be maintained by the entity as part of its compliance program:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies, Procedures and Documentation Requirements

Section 13401 of the HITECH Act provides that the administrative safeguards provisions of the HIPAA Security Rule apply to "a business associate of a covered entity in the same manner that such subsections apply to the covered entity." HITECH § 13401(a). The law requires that the security provisions be incorporated into the business associate agreement between the business associate and the covered entity. Further, the HITECH Act mandates for the first time that business associates also must enter into business associate agreements with other business associates.

If you have a question about this or any healthcare issue, please contact:

Jason C. Furedy	602.262.5322	JFuredy@LRLaw.com
Gregory Y. Harris	602.262.0218	GHarris@LRLaw.com
Roy W. Kyle	520.629.4466	RKyle@LRLaw.com
Matthew C. Sweger	520.629.4431	MSweger@LRLaw.com

Administrative Safeguards Standards

The provisions of the Security Rule which have been made applicable to business associates include the administrative safeguards standards 45 C.F.R. § 164.308. This Rule requires covered entities (and now business associates in light of the changes to the HITECH Act) to satisfy a number of specifications. These provisions are further explained below.

For instance, the Rule requires that the entity have a security management process in place to "implement policies and procedures to prevent, detect, contain and correct security violations." 45 C.F.R. § 164.308(a)(1)(i). The implementation specifications require an entity to conduct an analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic health information. 45 C.F.R. § 164.308(a)(1)(ii)(A). In addition, the entity must undertake a risk management analysis and implement measures "sufficient to reduce risks and vulnerabilities to a *reasonable and appropriate level* to comply with section 164.306(a)." 164.308(a)(1)(ii)(B) (emphasis added). The Rule does not define the "reasonable and appropriate" standard, and instead leaves this interpretation to the context in which the analysis is undertaken. The Rule also requires the entity to have a sanctions policy in place, similar to that required under the HIPAA privacy rule, that applies appropriate sanctions against workers who fail to comply with the entity's security policies and procedures. 45 C.F.R. § 164.308(a)(1)(ii)(C). Further, the security management process requires the entity to have a system in place to "regularly review records of information system activity, such as audit logs, access reports and security incidence tracking reports." 45 C.F.R. § 164.308(a)(1)(ii)(D).

The Security Rule also requires the entity to have an assigned security official. The entity must identify the person responsible for the development and implementation of the policies and procedures established under the administrative safeguards standards. 45 C.F.R. § 164.308 (a)(2). The safeguards standards also require that workforce security rules be adopted. In general, the entity must have policies and procedures to address workforce access to electronic health information and to prevent inappropriate access to this information. The entity needs to include procedures which address how people gain access to protected information, the supervision of these individuals, and the locations from which the information may be accessed. 45 C.F.R. § 164.308(b)(3)(i)(A). Further, the Rule supports the entity's adoption of procedures to determine who should have access to information. 45 C.F.R. § 164.308(b)(3)(i)(B). Finally, the Rule also suggests the procedures concerning the termination of access when a person leaves the workforce or no longer holds a position where access is appropriate. 45 C.F.R. § 164.308(b)(3)(i)(C).

The administrative safeguards standards also address the authorizations and management of access to PHI. 45 C.F.R. § 164.308(a)(4)(i). The standards require the entity to have a process in place to assess the means of granting and establishing, documenting, reviewing, and modifying user rights and work station access to PHI. 45 C.F.R. § 164.308(a)(4)(ii)(B) and (C).

In addition, the Rule requires security awareness and training. 45 C.F.R. § 164.308(a)(5)(i). The Rule establishes specifications for the use of periodic security updates, software to guard against, detect, and report malicious software, monitor login attempts, including failed attempts or other discrepancies and password management. 45 C.F.R. § 164.308(a)(5)(ii). The Security Rule also requires the entity to have in place a process to address security incidents. This required standard, which now must be read together with other provisions of the HITECH Act with respect to how the entity must handle security breaches, provides that the security plan must include steps to "identify and respond to suspected or known security incidents; mitigate, to the extent practical, harmful effects of security incidents that are known to the covered entities; and document security incidents and their outcomes." 45 C.F.R. § 164.308(a)(6). Similarly, HITECH Act Sec. 13402(f) require an entity to provide notice of a breach, which must include a description of the breach, a description of the information taken, steps that individuals should take to protect themselves, a description of the steps taken to investigate, mitigate, and protect against future breaches, and contact information within the company about the breach.

The entity also must have policies and procedures for contingency plans to protect information loss due to emergencies such as error, theft, system failure, and natural

disasters. 45 C.F.R. § 164.308(a)(7)(i). The Rule also prescribes three required specifications for data backup, disaster recovery, and emergency mode operations. 45 C.F.R. § 164.308(a)(7)(ii)(A), (B), (C). Finally, the Rule also suggests that entities periodically test and revise their procedures.

The Rule also establishes a separate standard governing business associate agreements. The safeguards standard allows covered entities to enter into business associate agreements which permit business associates to share protected health information with others on behalf of the covered entity if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard that information. 45 C.F.R. § 164.308(b)(1). A covered entity must obtain assurances that business associate will implement required safeguards to appropriately protect the information and that individuals with which the business associate deals will in turn agree to implement reasonable and appropriate safeguards to protect information, including to:

- Report security incidents to the covered entity.
- Authorize termination of the agreement in the event of a breach.

45 C.F.R. § 164.314(a)(2).

Physical Safeguards Standards

The HITECH Act also incorporates the physical safeguards standards for information security. Under this element of the Rule, covered entities and business associates must have policies and procedures that address facility access controls, work station usage, work station security, and device and media controls. With respect to the facility access control standards access, must be controlled "while ensuring that properly authorized access is allowed." 45 C.F.R. § 164.310(a)(1). The implementation specifications require the adoption of policies for continued access to the data in the event of an emergency, a security plan to prevent unauthorized access or theft of hardware, to control visitor access to the property, and to require the retention of maintenance records. 45 C.F.R. § 164.310(a)(2). The work station use standard requires the adoption of policies and procedures which specify the work stations that are to be used, the manner in which the work stations are to be used, who may use the work stations, and rules concerning the physical surroundings in which work stations will be used to access electronic protected health information. 45 C.F.R. 164.310(b).

The device and media control standard addresses policies and procedures governing the receipt and removal of hardware and other electronic media that contain protected information. The Rule imposes standards governing how the entity will dispose of its devices as well as standards governing how devices can be reused. 45 C.F.R. § 164.310(d)(2)(i) and (ii). The Rule also requires that standards be adopted regarding the maintenance of records concerning the movement of hardware and electronic media as well as maintenance for data backup and storage of information contained on these items. 45 C.F.R. § 164.310(d)(2)(iii) and (iv).

Technical Standards

Section 45 C.F.R. 164.312 establishes the "technical safeguards" that covered entities and business associates must satisfy. These standards require the implementation of access controls that permit—and limit—access only to those persons or software programs that have been granted access rights to the PHI. Entities must assign unique identification to each user to identify and track use of PHI and must establish emergency access procedures. Entities may provide for automatic logoffs and may implement systems to encrypt and decrypt data. Entities must implement audit controls and policies and procedures to protect data integrity to guard against improper alteration or destruction, to authenticate data access, and to provide for transmission security.

Organizational Safeguards

The Security Rule imposes "organizational requirements" on covered entities and business associates under 45 C.F.R. § 164.314. These standards impose a standard that holds the entity liable for a pattern of conduct that the entity knew about that constituted a material breach or violation of the business associate's obligation unless the entity took steps to prevent or end the violation or the entity terminated the agreement, or if termination could not feasibly be accomplished, reported the breach to HHS. The covered entity and the business associate must enter into

written business associate contracts that implement the administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the electronic protected health information. The agreement must implement reasonable and appropriate safeguards to protect PHI. The entity must agree to report to the covered entity any security incident of which it becomes aware. Finally, the agreement must authorize its termination if the covered entity determines that the business associate has violated a material term of the contract.

Implementation of the Privacy Rules

HITECH Act Section 13404 provides that business associates are subject to the same obligations as covered entities in terms of the duty to safeguard PHI. The act mandates that the privacy standards established by the privacy rule must be incorporated into business associate agreements. The section also permits penalties to be imposed directly against business associates for a violation of the standards by a business associate.

New "Rights" created by the HITECH Act

The HITECH Act establishes two significant changes that impact individuals and PHI. Before the HITECH Act, individuals could request special treatment of PHI—and refuse release of information to a third party—even for treatment, payment or health care operations—and a covered entity could agree to the request—or not. Under the HITECH Act, a covered entity must comply with the requested restriction if the disclosure would be to a health plan for purposes of carrying out payment or health care operations—but not for treatment; and the PHI pertains solely to a health care item or service for which the health care provider involved has been fully paid by the patient. HITECH Act Sec. 13405(a)

The Act creates broader "accounting" rights that allow an individual to be informed of disclosures by a covered entity or business associate of PHI. Under the rules in place before the enactment of the HITECH Act, entities had no obligation to provide an accounting of disclosures made for "treatment", "payment" or "health care operations". Under the HITECH Act, if the entity maintains electronic health records, then the entity's accounting must keep a log of PHI disclosures made for treatment, payment or health care operations. HITECH Act Sec. 13405(c).

Enforcement

Section 13410 of the HITECH Act specifically empowers a state attorney general to enforce HIPAA. This authority did not previously exist. This section also increases the range of potential penalties for violations of HIPAA as follows:

- $100 for each violation in which it is established that the person did not know (and by exercising reasonable diligence would not have known of the violation), except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.
- $1,000 for each violation due to reasonable cause and not to willful neglect, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $100,000.
- $10,000 for each violation due to willful neglect but which has been corrected, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $250,000.
- $50,000 for each violation due to willful neglect and which has not been corrected, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.

Conclusion

Businesses that handle protected health information for covered entities and covered entities that hire business associates face new obligations under HIPAA as a result of the enactment of the HITECH Act. So too for business associates that hire other business associates. This Client Alert outlines some important changes. A complete understanding of the new obligations created by the HITECH Act requires the study of the act in its original form.