TOPIC:

HITECH Act: New Law Requires Signific

Since their enactment in 2003 and 2005, respectively, the Privacy Rule and the Security Rule have affected significantly the way health information is handled, used and disclosed [9].

The Privacy Rule puts complex restrictions on how covered entities may use and disclose protected health information ("PHI") [10]. The Security Rule requires that covered entities protect health information [11] with administrative (e.g., policies and procedures), technical (e.g., using passwords to limit access to databases and audit trails to determine who has accessed data) and physical (e.g., requiring key cards to access data servers) safeguards. Violations of these Rules can result in civil penalties, criminal prosecutions, and private lawsuits [12]. Compliance is complicated further by the numerous overlapping state laws that govern health information, which in many cases are not preempted by HIPAA [13].

In addition to the increased costs associated with compliance with HIPAA, many colleges and universities have struggled with understanding the requirements of the HIPAA Rules and how they apply to institutional activities. Up until now, however, many institutions -- at least those without clinics or hospitals -- have avoided significant compliance costs because their primary roles are as business associates rather than as covered entities.

THE HITECH ACT CREATES SWEEPING NEW REQUIREMENTS THAT RAISE THE STAKES FOR COLLEGES AND UNIVERSITIES

The HITECH Act extends the reach of HIPAA, making it applicable directly to business associates as well as covered entities and also adds to the complexity of the Privacy Rule and Security Rule requirements. These dramatic changes can be summarized in four categories.

1. Business Associates Have Increased Obligations that Require Information System Upgrades and Enhanced Security Infrastructure

Business associates currently are not directly subject to HIPAA and instead are subject only to the fairly general privacy and security obligations imposed on them contractually in business associate agreements. The Act changes that balance of power, specifically imposing most Security Rule and many Privacy Rule obligations directly on business associates effective February 17, 2010. At the same time, the Act makes business associates directly subject to HIPAA civil and criminal enforcement and the accompanying penalties [14]. In many cases, these new obligations will, among other things, trigger the need for information systems changes (see numbered section 2 below).

The Act also requires the new obligations for business associates be included in business associate agreements, thus necessitating the renegotiation and amendment of college and university business associate agreements. When paired with the increased enforcement and liability risks (see numbered section 4 below) and the new restrictions placed on use and disclosure of PHI (see numbered section 2 below), these negotiations are likely to be contentious, requiring significant resources over a short time period.

One provision of the Act that may lead to more difficult negotiations of business associate agreements is the imposition directly on business associates of the obligation to terminate the business associate contract for material violations by the covered entity of that contract (absent cure by the covered entity) [15]. If termination of the business associate contract is infeasible, the business associate must report the violation to the Department of Health and Human Services ("HHS") [16]. With business associates now having the obligation to do something about covered entity breaches, business associates likely will demand additional representations and warranties from covered entities about their own HIPAA compliance.

The Act also clarifies that organizations such as Health Information Exchanges, Regional Health Information Organizations, and e-prescribing gateways [17] are business associates and are required to enter into business associate agreements with covered entity participants [18].

2. New Restrictions on Uses and Disclosures and Increased Individual Rights

The numerous modifications to the HIPAA Privacy and Security Regulations required by the Act create

additional burdens and restrictions that will require investment in new information systems, new business processes, and retraining of all relevant staff. The new requirements include the following:

Accounting of Disclosures . Existing HIPAA obligations to provide individuals with an accounting of disclosures have been expanded [19]. Covered entities will be required to keep a record, and provide an accounting to requesting individuals, of all disclosures made to third parties (including healthcare providers) for treatment, payment, and health care operations purposes when those disclosures are made through “electronic health records,” a term which is nom M[T]t

management or to recommend alternative therapies or providers [30]. With limited exceptions, the Act provides that for communications sent on or after February 17, 2010, a covered entity may not receive direct or indirect payment for making these otherwise permitted communications [31]. One limited exception provides that "reasonable" payment, to be defined by HHS in forthcoming regulations, is not prohibited if the communication relates to a drug or biologic currently prescribed for the recipient of the communication. This prohibition targets communications made by covered entities such as pharmacies, providers, and health plans when the communications are paid for by third parties, including pharmaceutical manufacturers.

De-identification. The Act specifies that HHS must iss ue guidance on or before February 17, 2010, on best practices for implementing HIPAA requirements for de-identifying PHI eÂco t fm

risk management strategy, and implement policies and procedures designed to ensure compliance.

Retrain Staff On The New Requirements. Covered colleges and universities should consider retraining all staff on the new requirements imposed on their organizations under the HITECH Act.

AUTHORS:

Barbara Bennett, Partner, Hogan & Hartson, Washington D.C.

Alexander Dreier, Partner, Hogan & Hartson, Washington D.C.

Candace Martin, Associate, Hogan & Hartson, Washington D.C.

RESOURCES:

Statutes and Regulations:

HIPAA, Pub. L. No. 104-191 (Aug. 21, 1996).
ARRA, Pub. L. No. 111-5 (Feb. 17, 2009).
HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E.
HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C.

NACUA Resources:

HIPAA Resource Page

Additional Resources:

Health Information Privacy Website, OCR.
Summary of Health Privacy Provisions, Center for Democracy & Technology.

FOOTNOTES:

FN1. American Recovery and Reinvestment Act of 2009 ("ARRA"), Pub. L. No. 111-5, 123 Stat. 115 (Feb. 17, 2009)

FN2. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

FN3. A covered entity is defined under HIPAA as (1) a health plan; (2) a health care clearinghouse; and (3) a health care provider who transmits any health information in electronic form in connection with certain transactions. 45 C.F.R. § 160.103 (2006). Clinics or counseling centers are covered entities only if they bill payers electronically.

FN4. Business associate agreements can also include providing wellness, fitness center, EAP management or other services to the covered health plans of local employers. Another example would be creating and/or managing a health information database for external covered entities. A business associate is defined as "a person who (1) on behalf of.[a] covered entity or of an organized health care arrangement…in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information…or any other function or oan

FN16. The reciprocal of this obligation is currently imposed on covered entities with respect to business associate breaches. 45 C.F.R. § 164.504(e)(1)(ii).

FN17. These terms are not statutorily defined. In general, a regional health information organization is an organization that unites health care stakeholders within a defined geographic area and oversees health information exchange among the organizations for the purpose of improving health care within that particular geographic community. A health information exchange is the electronic movement of health information among organizations based on nationally recognized standards. The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology,

FN25.

covered entity involved in the breach on its website.

FN36. ARRA § 13402.

FN37. 74 Fed. Reg. 19,006 (Apr. 27, 2009).

FN38. ARRA § 13407. A PHR vendor is defined as an entity, other than a covered entity, that offers or maintains a personal health record. ARRA § 13400(18). Recent guidance from the FTC also makes clear that PHR vendors exclude business associates. PHR related entities include entities that offer products or services through the website of a PHR vendor or a HIPAA covered entity, or access information in a PHR, or send information to a PHR. A college or university that offers an online health record through its benefits office or through private-labels, such as Google or Microsoft PHRs (rather than through its health plan), could be subject to this breach provision.

FN39. Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009). The Act also directs the FTC and HHS to study and submit a report to Congress on the imposition of privacy and security requirements (to replace and/or expand the temporary breach requirements in the Act) on entities that are not HIPAA covered entities or business associates, including PHR vendors and their contractors. ARRA § 13424(b).

FN40. In particular, a state attorney general is now authorized to bring a civil action in federal district court in cases where the attorney general believes that the interests of its state's residents are threatened or adversely affected by a person who violates the HIPAA Privacy or Security Rules. The state attorney general must provide notice to the Secretary of the intent to bring a civil action and the Secretary has the right to intervene, to be heard, and to file petitions for appeal. A state attorney general may seek statutory damages, injunctive relief, and attorneys' fees, but cannot institute an action if the Secretary has already done so. ARRA § 134010(e).

FN41. The ARRA provisions requiring HHS to audit covered entities and their business associates are effective February 17 2010. It is anticipated that HHS will use contractors to conduct the required audits of covered entities and their business associates.

FN42. ARRA § 134010(d).

FN43. Monies collected for enforcement of a privacy and security violation under the HITECH Act or HIPAA are required to be used by OCR for further enforcement, and within three years a methodology must be adopted for distributing a percentage of those monies to individuals harmed by the violations, providing

resources for enforcement and an incentive for individuals to report violations. ARRA § 13410(c)(1).

FN44. ARRA provides that HIPAA's criminal penalties may be imposed against individuals, including, but not limited to, employees who obtain or disclose individually identifiable health information without authorization, provided that the information is maintained by a covered entity. ARRA § 13409.

FN45. The plain language of the HITECH Act provides that certain (but not all) of the new business associate obligations must be incorporated into business associate agreements, but no guidance is provided to confirm whether that requirement (i) is intended to apply only to business associate agreements entered into on a going-forward basis, or (ii) is intended to mean also that existing business associate agreements must be amended.