NACUANOTES
July 17, 2009
Volume 7 No. 9

TOPIC:

HITECH Act: New Law Requires Significant Investment in Health Information Privacy and Security

INTRODUCTION:

On February 17, 2009, the stimulus law, the American Recovery and Reinvestment Act of 2009 ("ARRA") [1], was enacted. Title XIII of the ARRA, The Health Information Technology for Economic and Clinical Health Act ("HITECH Act" or the "Act"), imposes new federal security breach notice requirements and adds numerous new privacy and data security restrictions for covered entities and their business associates under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") [2].

Many provisions of the Act directly impact colleges and universities that:

- Have medical clinics, counseling centers, physicians and other providers and facilities that are covered entities under HIPAA [3]
- Are business associates of covered entities, such as medical or public health schools that provide certain services to hospitals, clinics or state healthcare programs [4]
- Sponsor employer health plans that are self-insured [5]

The most significant challenges posed by the Act are:

- Business associate agreements will be subject to potentially contentious renegotiation and amendment
- Compliance may require investment in new information systems and applications
- Compliance will require new business processes and retraining of all affected staff

The costs of compliance, much of which will need to be incurred by February 2010, may be substantial for many institutions [6].

This Note provides a brief overview of the requirements of the Act and the challenges faced by colleges and universities subject to it. It presumes readers have a working knowledge of HIPAA's privacy regulations ("Privacy Rule") [7] and security regulations ("Security Rule") [8].

DISCUSSION:

Background

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 not well defined in the Act [20]. In addition to accounting to an individual for disclosures, covered entities may require their business associates to account directly to the individual for disclosures made by the business associate on the covered entity's behalf. HHS is directed to promulgate regulations to assist with the implementation of these new requirements, which are scheduled to go into effect in either 2011 or 2014, depending on the date on which the covered entity acquired the electronic health record at issue [21], but there are additional provisions that allow HHS to delay these effective dates by two more years. Nonetheless, compliance is likely to require systems and process changes for colleges and universities [22].
- ***Minimum Necessary Disclosures***. The Act puts increased emphasis on, and additional teeth behind, the requirement that a covered entity must limit uses and disclosures of PHI (both for internal operations and in disclosing PHI to a third party) to only that information that is the "minimum necessary" to effect the intended purpose of the use or disclosure [23]. In addition to imposing this minimum necessary obligation directly on business associates, the Act requires HHS to issue guidance on what constitutes "minimum necessary" information for a permitted use or disclosure [24]. Until such guidance is released, the Act creates a "safe harbor" by providing that use or disclosure of a "limited data set," which is PHI with all direct identifiers removed (i.e., essentially de-identified data with dates and zip codes added back in), will be deemed the minimum necessary. If more than a limited data set is disclosed, the covered entity or business associate disclosing the PHI should first have made and documented the determination that the PHI to be disclosed is the minimum necessary to achieve the intended purpose. These new requirements are effective February 17, 2010. Because many systems are not capable of controlling data access to the granular level needed to limit that access to the minimum necessary or limited data set, the Act effectively creates a need for investment in new systems and processes.
- ***Right to Restrict Disclosures to Health Plans***. Under current HIPAA provisions, individuals may request restrictions on permitted disclosures of their PHI, but covered entities are not required to agree to any request [25]. As of February 17, 2010, the Act now requires that covered entities must comply with requests by individuals not to disclose PHI to a health plan for payment or health care operations purposes if the PHI relates solely to an item or service for which the provider has been paid out of pocket in full [26]. Processes will need to be put in place to handle this new requirement [27].
- ***Right to Obtain Electronic Copies of Records***. An individual's right to obtain a copy of his or her medical records when such records are maintained by the covered entity in an electronic health record is expanded as of February 17, 2010 to include the right to obtain a copy in electronic format, and to direct that the covered entity transmit the copy to an entity or person designated by the individual [28].
- ***Prohibition on Remuneration in Exchange for PHI***. Currently, if a covered entity is permitted to disclose PHI to a third party, nothing prohibits the covered entity from receiving payment or other value in exchange for the disclosure. With limited exceptions, the Act prohibits covered entities from receiving direct or indirect remuneration in exchange for PHI without individual authorization [29]. Limited exceptions include for treatment and for public health activities and research, but any remuneration received in exchange for PHI for research may be limited to the cost of preparation and transmission of the data. HHS is directed to issue initial regulations on or before August 17, 2010, and compliance is required six months after final regulations.
- ***Limitations on Marketing to Individuals***. Communications that encourage the use or purchase of a product or service are permitted without an individual authorization, and covered entities can be paid for making the communications, if they are (i) about products and services included in the individual's plan of benefits or available only to health plan enrollees, (ii) for treatment purposes, or (iii) for care

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 issue guidance on or before February 17, 2010, on best practices for implementing HIPAA requirements for de-identifying PHI [32]. For colleges and universities that de-identify data or use de-identified data, the new guidance may require an overhaul of the methodologies used for the de-identification or place additional restrictions on those methodologies.

3. Federal Security Breach Notification Requirements

Incidents of unauthorized access or acquisition of personal data, including patient data, have increased significantly the last few years, resulting in laws in most states that require that individuals be provided written notice of these security breaches. Most of these state laws do not apply to a security breach involving health information that does not include certain information such as a social security number or driver's license number or that is encrypted. These notice requirements have created a high public profile for businesses that have had security breaches.

The HITECH Act creates new federal security breach notice laws that apply to all personal information held by colleges and universities in their roles as covered entities, business associates, and vendors of personal health records (including those made available to employees). These laws require notice to individuals, government agencies, and, in some cases, the media.

For Covered Entities and Business Associates. The Act creates a new federal security breach notification law that applies to covered entities and their business associates and that goes into effect 30 days after HHS issues regulations, which are required to be issued on or before August 17, 2009 [33]. In addition to notifying individuals of the breach [34], the law requires reporting of all qualifying breaches to HHS, which will publicly post the information for certain breaches [35]. In cases in which more than 500 individuals are affected, the media also must be notified. The Act specifies detailed requirements regarding the content, timeliness, and methods of providing notice [36]. Because this federal law does not preempt State security breach notification laws, covered entities still must also comply with similar state laws.

A safe harbor against required notification exists for information that has been secured by technology that renders the PHI "unusable, unreadable or indecipherable" to unauthorized individuals. HHS recently issued guidance providing that encryption and destruction are the only two methodologies that are currently deemed to secure information. Notice is not required if the information subject to unauthorized acquisition was so rendered [37]. HHS will issue periodic guidance on other qualifying methodologies.

For PHR Vendors and their Contractors. The Act also includes separate and temporary security breach notification requirements for non-HIPAA covered vendors of personal health records ("PHRs"), PHR related entities, and their contractors [38]. These entities are required to notify affected individuals and the Federal Trade Commission ("FTC"), which in turn must notify HHS of any breaches of health care data. The FTC may take action under Section 5 of the FTC Act for unfair and deceptive trade practices. On April 16, 2009, the FTC issued notice seeking public comment on a proposed rulemaking in connection with these requirements [39].

4. Strengthened Enforcement and Increased Penalties

Since 2003, when compliance with the Privacy Rule was first required, government enforcement of the HIPAA rules has been almost non-existent, lulling many institutions subject to those laws into complacency. This will no longer be the case. Government agencies, plaintiffs' attorneys, and individuals now have attractive incentives and mandates for aggressive enforcement, which raises the stakes for colleges and

universities and their employees with respect to compliance.

State AGs may enforce HIPAA. Before, HHS Office for Civil Rights and the Justice Department were the only HIPAA enforcement authorities. Now, state attorneys general are provided with specific limited enforcement power under the Act with respect to HIPAA violations, effective immediately [40].

Penalties are increased and HHS audits required. To date, HHS largely has worked with covered entities to correct the HIPAA violations that have come to the attention of HHS and has mostly refrained from levying monetary fines. The Act now requires HHS to audit covered entities and their business associates rather than just respond to violations brought to its attention [41]. Also, effective immediately, the Act adopts a tiered civil monetary penalty structure for HIPAA violations that increases the penalty amounts for violations (up to an annual maximum of $1.5 million for uncorrected violations based on willful neglect) and has the potential to significantly change the way HIPAA is enforced by HHS [42]. And while the Act specifically allows for corrective action in lieu of penalties for cases in which the person did not know and did not have reason to know about the violation, penalties are now required to be imposed in other cases.

Willful neglect violations must be investigated and resources are provided for enforcement. Other enforcement provisions take effect in the future. Provisions that (i) require investigation of violations that indicate willful neglect, (ii) require penalties for those violations, and (iii) allow the Secretary of HHS to impose civil monetary penalties for criminal cases that the Justice Department has declined to prosecute are to take effect in February 17, 2011, and shall be the subject of regulations to be issued on or before August 17, 2010 [43].

Individuals may be criminally liable. The Act also clarifies that criminal penalties may be imposed on individuals, including but not limited to employees of covered entities or business associates, for HIPAA violations [44].

5. Other Requirements

In other provisions, the Act also addresses the use of PHI for fundraising, the definition of psychotherapy notes, the establishment of HHS education and assistance outreach efforts, and required studies and reporting to Congress. The Act also confirmed that the current state of the law with respect to HIPAA preemption of state law is not changed.

6. Compliance Challenges

In addition to the sheer volume of new requirements that colleges and universities face as covered entities, business associates, and PHR vendors, compliance with the Act demands significant new investment in IT hardware; software changes; substantial changes in business processes, policies and procedures; and retraining of staff. These challenges come at a time when resources already are scarce and will require colleges and universities to make difficult decisions about resource/risk trade-offs.

7. Recommended Steps

- ***Prepare For New Breach Requirements.*** The new breach provisions are likely effective in September 2009. Colleges and universities covered under the new breach provisions can prepare in advance for the new requirements by educating affected staff and putting compliance processes in place to respond to any breaches that may occur.
- ***Address New Business Associate Requirements.*** To address the new business associate requirements, covered colleges and universities may wish to consider developing a new, revised business associate agreement form template. Covered colleges and universities should also be mindful of issues that may arise during negotiation or renegotiation of business associate agreements and determine when and if to renegotiate existing business associate agreements [45].
- ***Perform a Security Risk Assessment.*** Under the new requirements, business associates are now subject to most of the requirements of the HIPAA Security Rule. As part of their compliance efforts, covered colleges and universities should perform a security risk assessment that evaluates and documents how it is in compliance with the Security Rule standards and specifications, determine a

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 activity regulated by…[HIPAA]; or (2) provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation…, management, administrative, accreditation, or financial services to or for…[a] covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person." 45 C.F.R. § 160.103. Not all relationships with hospitals are business associate relationships. Some medical school physicians are part of an organized healthcare arrangement with the hospital in which they practice medicine and these physicians may be subject to HIPAA as a covered entity. The business associate standard does not apply to disclosures by a covered entity to a health care provider concerning treatment of an individual. 45 C.F.R. § 164.502(e)(1)(ii)(A).

FN5. Under HIPAA, health plans are covered entities. Employers that sponsor health plans are responsible for the plans' compliance with HIPAA. Employers also often enter into business associate agreements with third party administrators ("TPAs") or others that provide services to the health plans.

FN6. The new privacy and security requirements impose various compliance deadlines. Colleges and universities subject to the new requirements should carefully review all of the relevant requirements and their effective dates.

FN7. 45 C.F.R. Part 160 & Part 164, Subparts A and E.

FN8. 45 C.F.R. Part 160 & Part 164, Subparts A and C.

FN9. In addition to the Privacy and Security Rules, the HIPAA Administrative Simplification Regulations also include the following regulations -Transaction and Code Set Standards, Identifier Standards, and the Enforcement Rule.

FN10. Protected health information means "individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium." Protected health information excludes individually identifiable health information in education records and other records that are covered by (or excluded from) the Family Educational Rights and Privacy Act and employment records held by a covered entity in its role as employer. 45 C.F.R. § 160.103.

FN11. Health information means any information, whether oral or recorded in any form or medium that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. 45 C.F.R. § 160.103.

FN12. The HIPAA statute does not provide a private right of action. However, plaintiff attorneys have used the statute as a privacy standard to support related causes of action.

FN13. *See generally* ARK. CODE ANN. § 4-110-103(7) (2009); CAL CIV. CODE § 1798.82(e)-(f) (2008); P.R. LAWS ANN. tit. 10, § 4051 (2006). In addition, aside from health information, colleges and universities also have been subject the past few years to state data breach notice laws that require that written notices be sent to individuals when their personal information has been the subject of unauthorized access or acquisition. See, e.g., CAL CIV. CODE § 1798.82 (2008); FLA. STAT. § 817.5681(1)(a) (2009); NY GEN. BUS. LAW § 899-aa(2) (2009).

FN14. ARRA § 13401(a) and (b); ARRA § 13404(a) and (c).

FN15. ARRA § 13404(b).

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, *Defining Key Health Information Technology Terms*, Apr. 28, 2008.

FN18. ARRA § 13408.

FN19. Currently, the Privacy Rule provides individuals with a right to obtain an accounting for certain permitted disclosures of PHI made by or on behalf of a covered entity. The Rule however, exempts from this accounting requirement any permitted disclosures made for treatment, payment, and health care operations (TPO) purposes.

FN20. ARRA § 13405(c)(1); *see also* definition of "electronic health record" ARRA §13400(5).

FN21. ARRA § 13405(c)(4).

FN22. System and process changes are likely given that colleges and universities subject to the new privacy requirements will now be required to account for TPO disclosures. Thus, covered colleges and universities will need new system and process efforts to capture all the TPO disclosures that are not now captured or documented. Presumably this includes all disclosures of (or incidents of access to) PHI that occur internally within a covered entity or business associate organization; thus, capturing and documenting all these could be a significant burden. Perhaps HHS will more reasonably limit the application of this new requirement in its regulations.

FN23. ARRA § 13405(b).

FN24. ARRA § 13405(b)(1)(B).

FN25. 45 C.F.R. § 164.522(a)(1)(i)(A).

FN26. ARRA § 13405(a).

FN27. These may include providing notice to individuals of their new rights, establishing processes to comply with individual requests not to further disclose such information, ensuring that information is not disclosed to health plans prior to the time at which the individual may exercise this right, and so on.

FN28. ARRA § 13405(e).

FN29. ARRA § 13405(d)(1).

FN30. *See* definition of "marketing." 45 C.F.R. § 164.501.

FN31. ARRA § 13406(a)(2).

FN32. ARRA § 13424(c).

FN33. ARRA § 13402.

FN34. A "breach" is defined as the unauthorized access, acquisition, or disclosure of PHI that compromises the security or privacy of that information. ARRA § 13400(1). The law provides for limited exceptions to the definition of breach, including if the unauthorized person to whom information is disclosed would not reasonably have been able to retain it and including when the breach is unintentionally committed in good faith by an employee and the information is not further acquired, accessed, used, or disclosed.

FN35. If the unsecured PHI of 500 or more individuals is acquired or disclosed, HHS will identify the

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.