UNION OF AMERICAN PHYSICIANS AND DENTISTS

HIPAA AND THE NEW HITECH AMENDMENTS: WHAT IS REQUIRED AND HOW CAN PHYSICIANS COMPLY?

OCTOBER 22, 2010
Holiday Inn San Diego on the Bay
SAN DIEGO, CALIFORNIA

Presented by:
Karin M. Zaner[1]
Kane Russell Coleman & Logan PC
1601 Elm Street, Suite 3700
Dallas, Texas 75201
(214) 777-4203
e-mail address: kzaner@krcl.com

[1] This paper is almost entirely based on a paper authored by Jennifer Brownell, an associate at Kane Russell Coleman & Logan, PC. Her efforts in understanding and discussing this complex area of the law are truly appreciated.

HIPAA AND THE NEW HITECH AMENDMENTS: WHAT IS REQUIRED AND HOW CAN PHYSICIANS COMPLY?

Introduction.

HIPAA poses unique compliance challenges for physicians and those who receive protected health information from them. These challenges have considerably increased with the HITECH Amendments that were signed into law on February 17, 2009. One of the most important changes is that HITECH creates new requirements making the HIPAA privacy and security rules applicable to "business associates" of health care entities (which includes many types of third parties). How can physicians (who deal with protected health information on a daily basis) comply? Step one is understanding what the law provides. That is my topic today. Step two is creating procedures, policies, and forms to make compliance a part of the way that physicians practice. That important topic will be left for another day.[2]

Overview of HIPAA and HITECH.

HIPAA was enacted in August 1996 to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes." Pub.L. 104-191.

HIPAA required that the Secretary of the Department of Health & Human Services develop and publicize standards for the electronic exchange, privacy and security of health information. These standards are known as the *Administrative Simplification* provisions.

HIPAA also required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within three years of the Act's passage. Because Congress did not enact privacy legislation within the designated time, the Department of Health and Human Services ("HHS") developed regulations known as The Privacy Rule. The current version of The Privacy Rule can be found at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

The standards for protection of certain health information (termed "Protected Health Information" by the Act) set by HIPAA and the Privacy Rule apply to (1) health plans, (2) health care clearinghouses, and (3) health care providers (including physicians) who conduct certain financial and administrative transactions electronically (e.g., claim submission, billing, and fund transfers). *See* 45 C.F.R. § 164.104. The Privacy Rule refers to these parties as "covered entities." *See* 45 C.F.R. § 160.103. These Privacy Rule's health information protection standards

[2] Although not formally published, there has been some indication by the U.S. Department of Health and Human Services' Office for Civil Rights that the new requirements for business associates enacted under HITECH may not be enforced until "final regulations" are issued, which date is uncertain. *See* Attachment A. That said, efforts to comply with both HIPAA and HITECH need to be made as soon as possible.

extend to any business associate[3] that enters into an agreement, with a covered entity, concerning the use and disclosure of this information on behalf of the covered entity, and including required statutory provisions. *See* 45 C.F.R. §§ 164.502; 165.504(e).

Congress enacted the Health Information Technology for Economic and Clinical Health Act ("HITECH") as part of the federal stimulus bill signed into law on February 17, 2009. HITECH strengthens and expands HIPAA's privacy and security requirements but does not replace or amend them. HITECH is intended to build confidence and acceptance for increasing the use of Electronic Health Records by tightening HIPAA's requirements for the use, disclosure and protection of Protected Health Information.

HITECH directly regulates business associates of covered entities for the first time; making business associates criminally and civilly liable for any failure to comply with specified HIPAA security and privacy regulations. *See* HITECH §§ 13404, 13410. HITECH requires that business associates comply with HIPAA security rule provisions mandating administrative, physical and technical safeguards for protected health information. *Id*. at § 13404. It also requires business associates to adhere to terms of business associate agreements with covered entities, including restrictions on use and disclosure of protected health information. *Id*. Business associates are now obligated, under HITECH, to follow breach notification requirements when unsecured protected health information is breached. *See* HITECH §13402(b).

Business associates are required to comply with HITECH by February 17, 2010. HITECH's requirements for business associates related to certain HIPAA security and privacy regulations will require modification, revision or amendment of existing business associate agreements to ensure compliance with HIPAA and HITECH.

What is protected by HIPAA and HITECH?

HIPAA and HITECH aim to protect and secure certain individually identifiable health information that is classified by HIPAA as "Protected Health Information."

HIPAA, through Privacy Rule regulations, protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information ("PHI")." 45 C.F.R. § 160.103.

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

[3] In simplest terms, a "business associate" is a person to whom a covered entity discloses protected health information so the person can carry out, assist with, or perform a function or activity on behalf of the covered entity. *See, generally,* 45 C.F.R. § 160.103 at *Business associate*.

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. 45 C.F.R. § 160.103. Individually identifiable health information is a subset of health information that includes demographic information (e.g., name, address, birth date, Social Security Number). *See* 45 C.F.R. § 160.103.

Who is a business associate?

A business associate is a person to whom a covered entity discloses protected health information, so the person can carry out, assist with, or perform a function or activity on behalf of the covered entity. *See* 45 C.F.R. § 160.103 at *Business associate*. The business associate definition expressly includes a person who "provides, other than in the capacity of a member of the workforce of such covered entity, legal … services to or for such covered entity … where the provision of the service involves the disclosure of individually identifiable health information from such covered entity … or from another business associate of such covered entity … to the person." *Id*. at *Business associate* (1)(B)(ii).

When is a third party (such as a law firm or attorney) a business associate?

Based on the business associate definition, a third party is a business associate when it provides services to a covered entity where the provision of those services involves disclosure of individually identifiable health information from the covered entity to the third party.

Take the example of a law firm. To determine whether a law firm or attorney is a business associate, it must be determined (1) whether the lawyer or firm is obtaining individually identifiable health information from the covered entity, and (2) whether the lawyer or firm must disclose that information to provide its (or his or her) services to the covered entity. *See* 45 C.F.R. § 164.103 at *Business associate* (1)(B)(ii).

If an attorney or law firm is representing hospitals, healthcare entities, physicians, or other healthcare providers[4] in peer review proceedings or related litigation, they are likely business associates. These cases frequently turn on the underlying medicine, and an attorney will receive individually identifiable health information regarding patients The attorney represents these clients and provide legal services in hospital, administrative or judicial proceedings. In this context, the attorneys working on those cases appear to be business associates.

If an attorney or law firm represents healthcare entities, physicians or other healthcare providers in a medical negligence (healthcare liability) claim, wrongful death, survival claim, or other claim based on the covered entity's diagnosis or treatment, they appear also to be business associates. The covered entity clients are providing the attorney with individually identifiable health information for the plaintiff patient at issue in the claim, so that that attorney can represent

[4] A healthcare provider who electronically holds or transmits any health information in electronic form in connection with a transaction covered by HIPAA and its regulations is a covered entity. *See* 45 C.F.R. § 164.103 at *Covered entity* (3). Virtually all physicians are covered entities because they use electronic transmissions to transmit health information to insurance plans, healthcare clearinghouses, CMS and other third-parties involved in the collection, receipt and/or disbursement of payment for healthcare services.

them. Based on a review of HIPAA and HITECH, this appears to be true even if (1) the protected health information disclosed in the case is public record, (2) the individual whose protected health information is being disclosed is the plaintiff, and (3) the individual whose protected health information is being disclosed has authorized the client/covered entity to make the disclosure. The determinative factor is not whether others have access to the information but whether the covered entity client is making a disclosure of protected health information to that attorney, so that the attorney can provide legal services to the covered entity.

Moreover, if an attorney or law firm is providing compliance analysis, due diligence for a covered entity, risk management analysis, or any other legal service that would require a covered entity client to disclose to the attorney protected health information of individuals for use in providing those legal services, that attorney and law firm appear to be business associates.

These same analyses apply for third parties other than attorneys, such as third party experts and consultants.

What is a Covered Entity and a Business Associate required to do under HIPAA and HITECH?

- Comply with HIPAA privacy and security provisions by implementing necessary safeguards against a breach of an individual's PHI. *See* HITECH §§ 13401, 13404; 45 C.F.R. §§ 164.500 – 164.534 (The Privacy Rule); and 45 C.F.R. §§ 164.302 – 164.318 (The Security Rule).

- Comply with HIPAA and HITECH provisions, including incorporation of all pertinent regulations into Business Associate Agreements/Contracts. *See* HITECH §§ 13401(a), 13404(a); 45 C.F.R. §164.504(e).

- If a business associate, notify the Covered Entity with whom it has a Business Associate Agreement/Contract of any breach of an individual's unsecured PHI. *See* HITECH § 13402(b).

- If a covered entity, take required action after notification is given. *See* 45 C.F.R. § 164.404(c).

- Make policies and records regarding compliance with the Acts and any breach notification available to the Department of Health and Human Services for audit. *See* HITECH § 13411.

What constitutes a "breach" of PHI?

PHI is either "secured" or "unsecured."

Secured PHI is PHI that is secured in accordance with the Encryption Guidance standards set by the Department of Health and Human Services. *See* 74 Fed. Reg. 19006 (April 27, 2009) (defining standards for encryption of PHI to make it "secure"). PHI is considered unusable,

unreadable or indecipherable to unauthorized individuals if it has been encrypted or destroyed. If a covered entity or a business associate "secures" PHI in accordance with the Encryption Guidance standards, it can ultimately avoid the breach notification obligations. This is true even if there is an unauthorized use or disclosure of PHI. However, other notice obligations could apply, including any mandated by state privacy laws.

"Unsecured" PHI is "protected health information that is not secured by a technology standard that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization accredited by the American National Standards Institute." HITECH § 13402(h)(1)(B).

HITECH covers PHI maintained in any form – not just electronic data. Therefore, paper records containing PHI are subject to the HITECH breach notification provision. According to guidance from the Department of Health and Human Services, the only way to secure a paper record is to destroy it. Of course, doing so renders the record unusable. Therefore, as long as a PHI is maintained in paper form, it is unsecure. Electronic storage or transmission of PHI, which storage or transmission does not satisfy the Encryption Guidance would be unsecured. Covered entities and business associates must comply with the breach notification regulations when unsecured PHI is breached.

A breach is "the unauthorized acquisition, access, use, or disclosure of protected health information which comprises the security of privacy of such information, except where an unauthorized person to who such information is disclosed would not reasonably have been able to retain such information." HITECH § 13400(1)(A). These are very broad terms that encompass any unauthorized access use or exchange of PHI. It appears that the Department of Health and Human Services intends to interpret these terms by their plain meanings. *See* 45 C.F.R. § 160.103 (defining "use" as "sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information; and "disclosure" as "release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.").

An acquisition, access, use or disclosure of unsecured PHI will not give rise to a "breach" unless the acquisition, access, use or disclosure violates HIPAA's Privacy Rule. Further, a breach is a compromise that "poses a significant risk of financial, reputational, or other harm to the individual." 45 CFR § 164.402 at *Breach*(1)(i).

Per HITECH, a breach does not include: (1) unintentional acquisition, access, or use of protected health information by an employee or individual acting under authority of a covered entity or business associate if (a) the acquisition, access or use was made in good faith and in the course and scope of employment or professional relationship of the employee/individual with the covered entity or business associate, and (b) the information is not further acquired, accessed, used, or disclosed by any person; or (2) inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility and any such information received because of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person. HITECH § 13400(1)(B).

Further, HITECH is only concerned with breaches of PHI. If the breached information is not PHI, there is no breach.

Covered entities and business associates will need to perform a risk assessment when there is an unauthorized use or disclosure of PHI in their care to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. The Department of Health and Human Services identified a general but not exhaustive list of factors to be considered:

- Who impermissibly used the information and to whom was the information impermissibly disclosed?
- Whether any immediate steps were taken to mitigate an impermissible use or disclosure.
- Whether the PHI disclosed was returned before being accessed for an improper purpose.
- The type and amount of PHI involved in the disclosure.
- The risk of re-identification of PHI contained in a limited data set.

See 74 Fed. Reg. 42744-45 (Aug. 24, 2009). Other factors to be considered in assessing whether there is any significant risk of harm to the individual might include potential or anticipated harm to the affected individual's reputation, as well as the potential for harassment or prejudice as a result of the use or disclosure. It is important that the covered entity and/or business associate carefully analyze whether a breach requires notification. Notification of a breach when there is little to no risk of harm might create unnecessary concern and confusion.

When is a breach "discovered" and when must notice be given?

A breach is treated as discovered as of the first day on which the breach is known to the covered entity or business associate (including any person, other than the individual committing the breach, who is an employee, officer, or other agent of the business associate) or should reasonably have been known to the covered entity or business associate (or its person) to have occurred. *See* HITECH § 13402(c).

If discovered by a business associate, the business associate has 60 days from discovery of the breach to notify the covered entity about the breach. *See* HITECH §13402(d)(1). The covered entity's 60 day notification period runs from receipt of the business associate's notice of breach – unless the business associate is the covered entity's agent. *See* HITECH § 13402(c). In that case, the 60 day period runs from the business associate's discovery of the breach because the business associate is an agent of the covered entity and the associate's knowledge of the breach is imputed to the entity. *See id.*; *see also* 45 C.F.R. § 164.404(a)(2) (treating agent's knowledge of breach as covered entity's knowledge).

How does a covered entity give notification of a breach?

A covered entity is required to provide an affected individual with (1) a brief description of what happened – including date of breach and date breach was discovered, (2) a description of the types of unsecured PHI that were breached (e.g., social security number, birth date, home address, diagnosis, etc.), (3) steps the individual should take to protect himself from potential harm resulting from the breach (e.g., credit check), (4) a brief description of what the entity is doing to investigate the breach, mitigate harm, and protect against further breaches, and (5) contact procedures for individuals with questions or who want additional information – including a toll-free number, e-mail address, website or postal address. *See* 45 C.F.R. § 164.404(c).

How does a business associate give notification of a breach?

A business associate is obligated to notify the covered entity with whom it has a business associate agreement about any breach of the PHI for an individual whose PHI is the subject of the agreement. *See* HITECH §13402(b).

The business associate is not obligated to notify an affected individual or the Department of Health and Human Services of a breach of unsecured PHI. The covered entity bears that burden. *See* HITECH §§ 13402(a), (e)(3); 45 C.F.R. §164.408. However, the business associate's breach notification must identify each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed during the breach. *See* HITECH § 13402(b). The breach notification from the business associate to the covered entity must also include any other available information the covered entity is required to include in its notification to the individual, so the business associate should provide as much of this particular information as it can to the covered entity in its breach notice. *See* 45 C.F.R. § 164.410(c)(2).

What must be included in a Business Associate Contract?

A contract or "other arrangement" is required before a covered entity "may permit a business associate to create, receive, maintain, or transmit electronic protected health information" on its behalf. *See* 45 C.F.R. § 164.314.

Pursuant to HIPAA, the business associate contract must include provisions that (1) the business associate will "implement administrative, physical and technical safeguards that reasonably and appropriately protect" electronic PHI, (2) any business associate agent or subcontractor will also implement such safeguards, (3) the business associate will report "any security incident of which it becomes aware," and (4) the contract may be terminated for breach of any material term. *See* 45 C.F.R. § 164.314(a).

HITECH mandates that certain HIPAA Security Rule provisions, Privacy Rule provisions, and any additional HITECH privacy and security provisions be incorporated into business associate agreements/contracts.

The Security Rule.

The Security Rule is highly technical and codifies certain information technology standards and best practices for ensuring security of electronic PHI. *See* www.hipaasurvivalguide.com. Generally, the Security Rule requires implementation of three types of safeguards: (1) administrative, (2) physical, and (3) technical. *Id*. The guiding principal for the Security Rule is to "implement necessary safeguards." *Id*. However, it is difficult to define what is necessary.

Administrative safeguards are "administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's workforce [or, in compliance with HITECH, the business associate's workforce] in relation to the protection of that information." 45 C.F.R. § 164.304 at *Administrative safeguards*.

Physical safeguards are "physical measures, policies, and procedures to protect a covered entity's [and now a business associate's] electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." *Id*. at *Physical safeguards*.

Technical safeguards mean "technology and the policy and procedures for its use that protect electronic health information and control access to it." *Id*. at *Technical safeguards*.

HITECH mandates that Security Rule provisions in Sections 164.308,[5] 164.310,[6] 164.312[7] and 164.316[8] "shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. *See* HITECH § 13401(a). "The additional requirements of this title [HITECH] that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity." HITECH § 13401(a).

Under HIPAA and HITECH, to comply with the referenced Security Rule provisions, covered entities and business associates must:

- Implement policies and procedures to prevent, detect, contain and correct security violations;

- Identify the security official who is responsible for the development and implementation of administrative safeguard policies and procedures;

- Implement policies and procedures to ensure that only appropriate members of the workforce have access to electronic PHI;

[5] 45 CFR § 164.308: Administrative safeguards.
[6] 45 CFR § 164.310: Physical safeguards.
[7] 45 CFR § 164.312: Technical safeguards.
[8] 45 CFR § 164.316: Policies and procedures documentation.

- Implement policies and procedures for authorized access to electronic PHI that are consistent with the applicable requirements of the Privacy Rule;

- Implement a security awareness and training program for all workforce members (including management) – including security reminders, viruses, passwords and login monitoring;

- Identify and respond to suspected or known security incidents;

- Establish policies and procedures for responding to an emergency or other occurrence (*e.g.*, fire, vandalism, system failure, natural disaster) that could damage systems containing electronic PHI;

- Perform periodic and non-technical evaluations to ensure that standards continue to be met in response to operational and environmental changes;

- Implement policies and procedures to limit physical access to electronic information systems, while ensuring properly authorized access is allowed;

- Implement policies and procedures for workstation use, workstation security and device and media controls;

- Implement technical policies and procedure for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have appropriately granted access rights;

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI;

- Implement policies and procedures to protect electronic PHI from improper alteration or destruction;

- Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed;

- Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network;

- Require a business associate agreement/contract with covered entities, analogous to that required under the Privacy Rule that incorporates the business associate's obligations to provide administrative, physical and technical safeguards.

See 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316.

The Privacy Rule.

In general, the HIPAA Privacy Rule applies to covered entities and their usage and disclosure of PHI. Before HITECH, certain Privacy Rule provisions would apply to business associates who entered into a business associate agreement/contract with a covered entity. Now, under HITECH, Privacy Rule provisions continue to apply to business associates as do any new privacy regulations under HITECH.

Under HIPAA, a business associate may use and disclose PHI obtained pursuant to a business associate contract only in compliance with each applicable requirement of Section 164.504(e).[9] "The additional requirements of this subtitle [HITECH § 13404] that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate agreement between the business associate and the covered entity. *See* HITECH § 13404(a).

Under HITECH, a business associate is not required to comply in general with the Privacy Rule – it is required to comply with Privacy Rule requirements for business associate contracts and with any new HITECH provisions concerning privacy. *See* HITECH §§ 13404(a), (b). Thus, a business associate must comply with HITECH requirements for security breach notification, health plan PHI disclosure restrictions, new minimum necessary provisions, new EHR accounting of disclosure rules, new patient access to information rules, and new limitations on EHR sales and marketing. Further, the business associate's agreement or contract with a covered entity must incorporate these HITECH requirements as well as HIPAA provisions governing business associate agreements/contracts. *Id*.

A business associate is subject to penalties for failure to comply with business associate contract requirements under HIPAA and HITECH regulations – even if those provisions are not included, stated or incorporated in its business associate contract.

HITECH business associate contract compliance requires that the business associate:

- provide for permitted uses/disclosures[10] of PHI by the business associate on behalf of the covered entity;

[9] 45 CFR § 164.504(e): Privacy Rule business associate contract standard and specifications.

[10] In connection with such use and/or disclosure, HIPAA requires that the covered entity make reasonable efforts to limit PHI used or disclosed to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. 45 CFR § 164.502(b) (the "minimum necessary rule.)" HIPAA did not impose any such requirement on a business associate acting on behalf of a covered entity. But under HITECH, it appears that a business associate is required to abide by the "minimum necessary rule" and shall be treated as being in compliance with the "minimum necessary rule" with respect to use, disclosure or request of PHI only if the business associate limits such PHI to the extent practicable, to the limited data set (as defined by the Security Rule) or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively. HITECH § 13405(b). There are exceptions for use and disclosure required by law or for HIPAA compliance purposes. In the context of a health law practice, any analysis of what constitutes the "minimum necessary" use or disclosure of the PHI at issue will likely need to be determined on a case by case basis between the attorney and the physician-client/covered entity, considering what uses and disclosures will be required by law in the context of the physician's case. A business associate contract should incorporate provisions acknowledging the minimum necessary rule and

- prohibit uses and disclosures of PHI that are not permitted by the business associate contract or as required by law;

- use "appropriate safeguards" to prevent prohibited uses/disclosures of PHI – whether electronic, written or oral;

- ensure that any agent or subcontractor of the business associate agrees to the same conditions, restrictions as the business associate;

- make PHI available for individual access and amendment, and account for disclosures;

- make its internal practices, books and records available to the Department of Health and Human Services (and possibly the Office of Civil Rights) for review in determining the covered entity's compliance with HIPAA;

- provide for return, destruction or escrow of PHI upon termination of the business associate contract;

- authorize termination of the business associate contract if the covered entity determines the business associate has violated a material term of the contract;

45 CFR §164.504(e).

What penalties are available for violation of HIPAA/HITECH and who can enforce the Acts?

HITECH is intended to provide stricter enforcement of HIPAA's Privacy and Security Rule provisions, and to extend enforcement of those provisions to business associates. There are two types of penalties under HIPAA – civil and criminal. A HIPAA violation that is punishable as a criminal offense may not be grounds for civil penalties. *See* 42 U.S.C. § 1320d-5(b)(1). Criminal penalties under HIPAA are enforced by the US Department of Justice. Civil monetary penalties are enforced by the Department of Health and Human Services' Office of Civil Rights.

A covered entities and business associate that violate HIPAA are subject to both criminal and civil penalties. HITECH § 13404(c). Criminal penalties for HIPAA violation can only be imposed when there is proof beyond a reasonable doubt that the covered entity or business associate knowingly, and in violation of HIPAA or any of its regulations, uses or causes to be used a unique health identifier, obtains individually identifiable health information, or discloses individually identifiable health information to another person. *See* 42 U.S.C. § 1320d-6(a). The criminal penalties for violation of HIPAA include fines (ranging from not more than $50,000 to not more than $250,000 – depending on the degree of violation) and/or prison terms (ranging from 1 year to 10 years – depending on the degree of violation). *See id.*

---

setting out an agreement with the physician-client to determine what PHI is the minimum necessary to be disclosed and/or used under the case circumstances.

HITECH requires the Department of Health and Human Services to provide for periodic audits of compliance by covered entities and business associates. *See* HITECH § 13411. The Department must formally investigate a complaint if preliminary investigation of the facts indicates a possible HIPAA violation due to willful neglect. *See* HITECH § 13410(a)(2). A complaint must be in writing, name the covered entity or business associate, describe the conduct that constitutes a violation, and be filed within 180 days of the date the complainant knew or should have known of the conduct (unless the Department waives the time limit for good cause shown). *See* 45 C.F.R. § 160.306. Complaints will be investigated by the Office of Civil Rights, and can be informally resolved. *See* 45 C.F.R. § 164.312. If an informal resolution is not reached, the Office of Civil Rights may issue notice of proposed civil monetary penalties and the findings of fact on which such penalties are proposed. *See id.* A covered entity or a business associate can request a hearing on the proposed determination, with a formal hearing held before an administrative law judge. *See* 45 C.F.R. §§ 164.500 – 164.552. Any penalties imposed may not be challenged in court without following procedures to a final Department of Health and Human Services Appeals Board decision. *See* 45 C.F.R. § 164.548.

A covered entity and a business associate is required to give the Office of Civil Rights access to its records for a HIPAA compliance investigation or audit concerning a covered entity's compliance with HIPAA. *See* 45 C.F.R. § 164.504(e)(2)(ii)(H). There is no equivalent provision requiring access to a business associate's records to determine its compliance. However, it is likely the Office of Civil Rights will use formal routes to require such access if a business associate does not agree to informal access. Civil monetary penalties for failure to comply with HITECH requirements imposed on business associates range from (1) $100/violation to $25,000 maximum for an unknown violation in spite of due diligence, (2) $1,000/violation to $100,000 maximum for a violation due to "reasonable cause," or (3) $500,000/violation to $1.5 million maximum for a violation due to "willful neglect." *See* HITECH § 13410. The Department is required to publish regulations on what constitutes willful neglect, and is required to impose penalties for willful neglect beginning February 17, 2011. For now, the Department can impose civil monetary penalties for unknown violations and violations due to reasonable cause.

State attorneys general are granted jurisdiction to enforce HITECH and HIPAA, and can be awarded attorneys' fees for a successful action. *See* HITECH § 13410(e).

What is the relationship between HIPAA and HITECH and state laws?

While HITECH and HIPAA preempt contrary states laws (*see* 45 C.F.R. § 160.203; HITECH § 13421), neither preempts state laws that relate to privacy and security of individually identifiable health information. Covered entities and business associates charged with protection of individually identifiable health information under state law will need to comply with both the federal laws and any state law that offers more protection for health information.

Little guidance for compliance with HIPAA and HITECH

Unfortunately, neither HIPAA nor HITECH identifies what constitute best practices or minimum standards for business associate compliance; nor does either Act offer a sample business

associate agreement/contract. The Department of Health and Human Services has not yet issued any form business associate agreement/contract that would meet minimum standards under both Acts. Thus, defining best practices for compliance with both Acts will require the covered entity and business associate to review and understand both Acts and assess its existing practices, cost effective measures for compliance, and practical measures for compliance given the PHI it will be required to use and disclose on behalf of a covered entity.

Conclusion

Compliance under both HIPAA and HITECH will be complex and challenging for physicians and their business associates. Given the requirements and the possible penalties for noncompliance, prompt effort and attention must be paid to creating procedures and policies to make compliance a part of the way physicians practice medicine.

References used in this paper:

1. HITECH Act Text.
2. HITECH Act Effective Dates.
3. HIPAA Security Rule Summary and select Security Rule provisions.
4. HIPAA Privacy Rule Summary.
5. HITECH/HIPAA Business Associates Gap Analysis Checklist Version 2.1.
6. 74 Federal Register 42740: 45 CFR Parts 160 and 164 – Breach Notification for Unsecured PHI; Interim Final Rule (Monday, Aug. 24, 2009).
7. Lawyers in the Compliance Crosshairs: Avoiding New Penalties and Ethical Pitfalls When Using Health and Medical Information (Nov. 4, 2009 PowerPoint presentation authored by John R. Christiansen, J.D.).

847486v1(99902.00001.000)