Lawyers Beware: Take action now to protect healthcare information or risk stiff penalties!

By Jennifer A. Stiller
February 1, 2010

Starting this month, lawyers who represent clients in the healthcare industry face new statutory obligations to take affirmative steps to ensure the privacy of their clients' patient information when it is transmitted or stored electronically. Failure to meet these requirements could result in substantial financial penalties.

The new requirements were enacted as portions of the American Recovery and Reinvestment Act of 2009 (the economic stimulus legislation), which collectively are oh-so-cutely named the "Health Information Technology for Economic and Clinical Health Act" – or "HITECH Act."

Which attorneys are covered?

The new rules apply to attorneys who represent doctors, hospitals, health insurance companies, and any other person or entity that is considered a "covered entity" under the HIPAA patient privacy rules. (You'll find the definition of the term in 45 C.F.R. §160.103.) If the representation involves the attorney's having access to information that identifies one or more patients in any way, the attorney is considered to be a "Business Associate" of the covered entity, and takes on new responsibilities and liabilities under the HITECH Act.

It is generally safe to assume that any healthcare industry client is a HIPAA "covered entity." Under existing HIPAA regulations, covered entities are required to enter into a "business associate" agreement with any non-employee who "provides … legal … services to or for such covered entity where the provision of the services involves disclosure of individually identifiable health information…" 45 C.F.R. § 160.103.

Sophisticated clients such as hospitals and health insurance companies that have in-house lawyers generally have complied with this requirement, and your firm may already have several business associate agreements somewhere in your files. Less sophisticated clients may not have been aware of the requirement, so there may be no such existing agreement. (If there isn't such a contract, there should be, and unless your representation of the client is severely limited, you should advise them of this obligation.)

Tip: Not all lawyers are covered. The new rules do not apply to attorneys who merely interact with healthcare insurers or providers in the context of representing clients who are not themselves healthcare insurers or providers. For example, a personal injury lawyer who subpoenas a person's medical record, an estates lawyer drafting a medical power of attorney, or a business lawyer negotiating a deal between his non-healthcare client and a hospital or health insurance company would generally not be considered to be Business Associates.

OK, my law firm is a Business Associate. What's different this month?

The magic date is **February 17, 2010**. Whereas previously, if the law firm didn't live up to its contractual obligations concerning how patient information was to be handled, the worst thing it would face would be being fired by its client and possibly a suit for breach of contract. As of February 17, however, the law firm is *directly liable to the federal government* for having inadequate safeguards in place (regardless of whether private information is in fact compromised) – and the penalties for non-compliance can be stiff. These obligations will be enforced primarily by the Office of Civil Rights ("OCR") of the Department of Health and Human Services.

Specifically, effective February 17, the HITECH Act –

- Makes the core provisions of the HIPAA Security Regulations, which mandate administrative, physical, and technical safeguards to protect the privacy of electronically stored or transmitted health data, apply directly to Business Associates such as law firms;

- Applies new rules containing detailed requirements for disclosure of breaches of security, to Business Associates; and

- Authorizes OCR and the state Attorneys General to conduct direct enforcement activities against Business Associates with respect to these security requirements, as well as with respect to certain HIPAA Privacy Regulation requirements that are mandated for inclusion in BA Agreements.

What do I have to do?

First, it would be a good idea to pull out any existing BA Agreements you have with your clients and make sure you are complying with all of the obligations under them. Since BA Agreements have generally been drafted by healthcare lawyers mindful of adhering to the HIPAA Privacy Regulations, they should contain all the privacy requirements that will now be enforced directly against Business Associates such as your law firm. (If you want to check for yourself what those requirements are, check out 45 C.F.R. § 164.504(e).

Second, familiarize yourself with the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316, which are the Security Regulations requirements that apply directly to your law firm under the HITECH Act. (I call them the Core Regulations in this paper, and I'll discuss what they require below.)

Third, make a note of where to find the breach notification regulations, so that you can lay your hands on them easily if your firm should experience a breach of security of its electronic records. To make it easy for you, here's a link.

Fourth, ensure that your firm is meeting the requirements of the Core Regulations and prepare the required documentation.

Security obligations – a flexible approach

Three of the four Core Regulations that the HITECH Act applies to Business Associates describe administrative, physical, and technical safeguards aimed at protecting private healthcare information that is electronically stored or transmitted from being accessed by people not actually involved in treating the patient or conducting administrative activities relevant to that patient's treatment. The fourth prescribes obligations for the Business Associate to adopt policies and procedures and to document its activities.

All four regulations incorporate by reference a fifth regulation, 45 C.F.R. § 164.306, which states the underlying purpose of the HIPAA Security Regulations and explains some of the terminology used in the four Core Regulations.

Under the Core Regulations, the covered entity (and, by extension, the Business Associate) must –

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the Business Associate creates, receives, maintains, or transmits;

- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Regulations; and

- Ensure compliance with the HIPAA Security Regulations by its workforce.

The Core Regulations specify how this is to be done by setting forth standards that the Business Associate must comply with "in accordance with Sec. 164.306" (a phrase that introduces each one of the Core Regulations).

Fortunately, Section 164.306 takes into consideration that safeguards which might be appropriate in a large health insurance company or hospital, with hundreds of employees and its own IT staff, could be impractical or prohibitively expensive for a one-doctor physician practice or other small entity. Thus, Section 164.306(b) permits a covered entity (and by extension a Business Associate) to "use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications" set forth in the Core Regulations.

In deciding what is reasonable and appropriate, a covered entity/Business Associate must take into account the following factors:

- Your firm's size, complexity, and capabilities.

- Your firm's technical infrastructure, hardware, and software security capabilities.

- The costs of security measures.

- The probability and criticality of potential risks to electronic protected health information.

Subject to the flexibility described above, Business Associates *must* comply with the "Standards" set forth in the Core Regulations. "Implementation specifications" in the Core Regulations are categorized as either "Required" or "Addressable." Those designated as "Required" *must* be handled in the same manner as the Standards. For implementation specifications designed as "Addressable," the law firm must "assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information, and, as applicable to the firm —

- Implement the implementation specification if reasonable and appropriate; or

- If implementing the implementation specification is not reasonable and appropriate —

    (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

    (2) Implement an equivalent alternative measure if reasonable and appropriate.

With all this in mind, let's look at the Core Regulations.

Physical safeguards

The physical safeguards contain four Standards:

- **Facility access controls.** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

- **Workstation use.** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

- **Workstation security.** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

- **Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

The first of these Standards (Facility Access Controls) has four addressable implementation specifications. These deal with contingency operations (procedures that allow facility access in support of restoration of lost data in the event of an emergency); a facility security plan (to safeguard the facility and its equipment from unauthorized physical access, tampering, and theft); access control and validation procedures (to control and validate a person's access to facilities based on their role or function); and documentation of repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

> Tip: "Addressable". Remember that "addressable" implementation specifications don't give you a free pass. You still have to assess whether the specification is "reasonable and appropriate in its environment," considered in the context of its likely contribution to safeguarding the protected healthcare information in your firm's electronic files. If it is, you've got to implement it, and if it's not, you have to come up with an alternative approach, "if reasonable and appropriate." And you have to document your assessment and its results.

The last Standard (Device and Media Controls) contains two required and two addressable implementation specifications. Required: You must have (and follow) written policies and procedures addressing the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored, and you must implement procedures for the removal of electronic protected health information from reusable electronic media before the media are made available for reuse. Addressable implementation specifications concern procedures related to moving hardware and electronic media.

There are no implementation specifications for the other two Standards for physical safeguards.

Technical safeguards

The technical safeguards contain five Standards:

- **Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights. (See discussion of administrative safeguards below.)

- **Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

- **Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

- **Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

- **Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Tip: Encrypted e-mail. Here's how I'm handling it. My ISP is Verizon.net, which allows me to have several e-mail sub-accounts (such as families might use to have a separate e-mail account for each family member). I'm creating a new sub-account, set up for "data protection," which will cost me $4.99 a month. I'll also create a new address on my healthregs.com domain name, which I'll call confidential@healthregs.com. E-mail addressed there will come to me through the new, protected Verizon sub-account, and clients will be advised to send me information containing protected health information (as well as any other confidential information they wish to send me via e-mail) through that account only. E-mail sent to or from that account will be encrypted, and will require a password to open it.

The first Standard (Access Control) contains two required and two addressable implementation specifications. Required: You must assign a unique name and/or number for identifying and tracking user identity, and you must establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. Addressable implementation specifications under this Standard concern electronic procedures to terminate an electronic session after a predetermined time of inactivity, and a mechanism to encrypt and decrypt electronic protected health information.

The Integrity Standard contains one addressable implementation specification, which concerns implementation of electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Finally, the Transmission Security Standard has two addressable implementation specifications, which concern –

- Security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of; and

- Implementation of a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Tip: Internet fax services. If, like me, you use an internet fax service such as MaxEmail.com, check out your provider's mechanism for maintaining security of the data in the faxes you receive, and if your faxes currently arrive via unencrypted e-mail, make the appropriate adjustments.

Administrative safeguards

There are nine administrative Standards:

- **Security management process.** The firm must implement policies and procedures to prevent, detect, contain, and correct security violations.

- **Assigned security responsibility.** The firm must identify the security official who is responsible for the development and implementation of the HIPAA security policies and procedures.

- **Workforce security.** The firm must implement policies and procedures to ensure that all members of its workforce have appropriate access (as described in the Workforce Security administrative Standard) to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.

- **Information access management.** The firm must implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the HIPAA Privacy Regulations.

- **Security awareness and training.** The firm must implement a security awareness and training program for all members of its workforce, including management. (Before the thought of this causes dangerously high blood pressure in any senior partners, go back and reread the discussion of flexibility in administration of these regulations.)

- **Security incident procedures.** The firm must implement policies and procedures to address security incidents.

- **Contingency plan.** The firm must establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

- **Evaluation.** The firm must perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which the firm's security policies and procedures meet the requirements of the HIPAA Security Regulations.

- **Business associate contracts and other arrangements.** This Standard provides that a "covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate will appropriately safeguard the information." It is not clear at this point how this Standard applies in the case of Business Associates such as lawyers,

but absent clarifying regulations from OCR, the prudent course would be to substitute your firm's name for "covered entity" in this Standard and proceed from there.) The Standard does go on to say:

> A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and Sec. 164.314(a).

The Standard for Security Management Process includes four required implementation specifications. These are:

- *Risk analysis*. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by your firm.

- *Risk management*. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the requirements set forth on in the first bullet list on page 3.

- *Sanction policy.* Apply appropriate sanctions against workforce members who fail to comply with your firm's security policies and procedures.

- *Information system activity review*. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

The Workforce Security Standard has three addressable implementation specifications. These relate to procedures –

(1) For the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed;

(2) To determine that the access of a workforce member to electronic protected health information is appropriate; and

(3) For terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made under (2) above.

The Information Access Management Standard has one required and two addressable implementation specifications. The required specification relates to health care clearinghouse functions (see definition here), which is something law firms don't do. The addressable items concern policies and procedures for granting access to electronic protected health information (for example, through access to a workstation, transaction, program, process, or other mechanism), as well as policies and procedures that, based on the firm's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

The Security Awareness and Training Standard has four addressable implementation specifications that deal with periodic security updates, procedures for guarding against, detecting, and reporting malicious software, procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing, and safeguarding passwords.

The Security Incident Procedures Standard has one required implementation specification, which requires the firm to identify and respond to suspected or known security incidents, mitigate (to the extent practicable) harmful effects of security incidents that the firm knows about, and document security incidents and their outcomes.

The Contingency Plan Standard contains three required and two addressable implementation specifications. The required ones are:

- *Data backup plan*. Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

- *Disaster recovery plan*. Establish (and implement as needed) procedures to restore any loss of data.

- *Emergency mode operation plan*. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

The first addressable implementation specification relates to procedures for periodic testing and revision of contingency plans; the second one concerns assessment of the relative criticality of specific applications and data in support of other contingency plan components.

Finally, the Business Associate Contract Standard has one required implementation specification, which requires that the obligations of business associates must be set forth in a written contract.

Documentation requirements

To a large extent, the security requirements discussed above reflect IT professionals' consensus on what needs to be done to protect the security of *any* electronically stored or transmitted information. Given that lawyers are already subject to ethical requirements concerning client confidentiality, you may find that your firm already has similar safeguards in place. If so, that's terrific – but you're still not in compliance with the HITECH Act until you adopt policies and procedures and fulfill the documentation requirements set forth in 45 C.F.R. § 164.316.

There are two applicable Standards:

- **Policies and procedures.** Your firm must implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of just discussed, taking into

account the "reasonable and appropriate" factors listed on pages 3-4. The firm may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the HIPAA Security Regulations. The regulation describing this Standard also states that "[t]his standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of" the HIPAA Security Regulations.

- **Documentation.** The firm must –

  (1) Maintain in written form the policies and procedures implemented to comply with the HIPAA Security Regulations; and

  (2) If an action, activity or assessment is required by the regulations to be documented, maintain a written record of the action, activity, or assessment.

  In either case, the written documentation may be retained in electronic form.

The Documentation Standard contains three required implementation specifications, as follows:

(1) *Time limit*. Retain the documentation required by the Documentation Standard for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(2) *Availability.* Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(3) *Updates*. Review documentation periodically, and update as needed in response to environmental or operational changes affecting the security of the electronic protected health information.

Tip: Notice to clients. Particularly if you're a solo practitioner like me, you may be modifying some of your procedures to provide for secure transmission of data, such as the secure e-mail solution I've described previously. If participation in a secure data transmission requires client participation such as using a special e-mail address, be sure to notify your clients in the healthcare industry of the new procedures – and incorporate an explanation of them in your engagement letters with new clients.

Wow – this is a lot to do for a small part of our practice. What happens if we just let it slide?

It's not a good idea. In applying all of these requirements directly to Business Associates such as law firms, the HITECH Act (also known to the cognoscenti as "HIPAA on Steroids") substantially increases enforcement penalties and activities.

Previously, there was no affirmative government enforcement of the HIPAA patient-privacy and security requirements – only OCR's ability to investigate complaints. If a complaint revealed a violation, fines were limited to $100 per incident, with a maximum annual total of $25,000 for violations of the same requirement. There was no way that the patient whose private information was compromised could get monetary compensation.

Under HITECH –

- Civil money penalties increased to *as much as $50,000 per violation*, up to $1.5 million per year.

- Starting February 17, 2011, OCR is *required* to impose civil penalties if a violation is due to "willful neglect."

- OCR will keep the penalty money, to be plowed back into enforcement activities.

- OCR is directed to *conduct periodic audits* of covered entities and business associates to evaluate HIPAA compliance.

- State attorneys general are granted authority to bring civil actions to enforce HIPAA. (The Connecticut AG brought the first such action in mid-January 2010 against a managed care company that lost a non-encrypted external hard drive containing personal information for 1.5 million past and present customers. Articles on this case are here and here.)

- The Government Accountability Office is directed to prepare a report by August 17, 2012 recommending a methodology by which affected individuals can share in penalties collected for HIPAA violations. Once implemented, this will increase individuals' incentives to file privacy and security complaints, similar to the effect of the False Claims Act's "whistle-blower" provisions.

Conclusion

The requirements imposed by the HITECH Act have to do with protection of information that is stored or transmitted electronically. Law firms, more than most businesses, should already have taken steps to protect their data because of ethical obligations relating to confidentiality – so there is a decent possibility that much of what is required by the HIPAA Security Regulations has already been done.

Working through the requirements of the HIPAA Security Regulations and making sure that their requirements are appropriately addressed can be a useful exercise that can help us all bring our data security into line with the real risks that electronic data storage can expose us to.