Davis Wright Tremaine LLP

HHS Proposed Rules to Implement Privacy and Security Provisions of the HITECH Act

07.13.10

By Paul T. Smith, Adam Romney and Aleah Young Schutze

On July 8, 2010, the Department of Health & Human Services (HHS) released proposed rules that would modify the of the Insurance Portability and Accountability Act (HIPAA) privacy, security and enforcement rules to implement changes required by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The proposed regulations deal with the following topics:

Business Associates

- Expansion of the definition of business associate
- Application of the Security Rule
- Application of the Privacy Rule
- Contracts with subcontractors
- New requirements for business associate contracts
- Implementation of new contract requirements
- Penalties
- Responsibility of covered entities for violations by business associates

Privacy Rules

- Requests for special restrictions
- Minimum necessary use and disclosure
- Sale of protected health information
- Access to electronic health records
- Marketing
- Fundraising
- Decedents
- Research authorizations
- Immunization information
- Notice of privacy practices

Enforcement

Business Associates

Expansion of the definition of business associate

The proposed regulations would include the following as business associates:

- "Patient Safety Organizations" (PSOs), which are organizations that conduct patient safety and quality improvement activities under the Patient Safety and Quality Improvement Act of 2005 (PSQIA).
- Organizations that provide data transmission of protected health information (PHI) to a covered entity or its business associate, such as health information exchanges, e-prescribing gateways, regional health information organizations, and personal health-record vendors acting for covered entities.
- A covered entity's business associate subcontractors. These would be treated as business associates, except that the business associate contractor (rather than the covered entity) would be required to hold business associate agreements with its subcontractors.

Application of the Security Rule

Under the HITECH Act, business associates became subject to the administrative, physical, and technical security requirements of the HIPAA Security Rule (45 CFR § 164 Subpart C), as well as the requirements to maintain policies, procedures, and documentation of security activities. To implement these changes, the NPRM would insert the term "business associate" at appropriate points throughout the Security Rule, and make other conforming changes.

Application of the Privacy Rule

The HITECH Act does not make business associates directly subject to the HIPAA Privacy Rule (45 CFR § 164 Subpart E). Rather, it exposes business associates to HIPAA penalties if they violate the mandated terms of their business associate contracts. For example, a business associate is now liable for penalties if it makes a use or disclosure not permitted by its business associate contract.

To implement this change, the proposed rule would provide that a business associate may use or disclose PHI only as permitted or required by its agreements with the covered entity, or as required by law. It would also provide that a business associate may not use or disclose PHI in a manner that would violate the terms of the Privacy Rule if done by the covered entity (except for data aggregation and uses and disclosures for its own operational and legal compliance purposes, as currently permitted by the rule). Any other use or disclosure would now violate the Privacy Rule, as well as the business associate contract.

In addition, business associates would be required to disclose PHI:

- When required by the Secretary of HHS to investigate or determine the business associate's compliance with the rules; and
- To the covered entity, individual, or individual's designee, as necessary to respond to an individual's request for an electronic copy of PHI.

The NPRM also proposes extending the "minimum necessary" standard to business associates. Thus, a business associate would not be making a permitted use or disclosure under the Privacy Rule if it did not apply the minimum necessary standard, where appropriate.

Contracts with subcontractors

Under the Privacy Rule, a covered entity must include in its business associate contracts a requirement for the business associate to require subcontractors to agree to the same restrictions and conditions that apply to the business associate. The agreement need not be written. The proposed rule would require business associates to obtain full, written business associate contracts from their subcontractors. Covered entities would not be required to have business associate contracts directly with its subcontractors.

The proposed rule would require a business associate that became aware of a pattern or practice of activity of its subcontractor that constituted a material breach or violation of the subcontractor's contract to take reasonable steps to cure the breach or to terminate the contract, if feasible. In other words, a business associate would have to respond to breaches by its subcontractor in the same manner as a covered entity must respond to breaches by its business associate.

BACK TO PAGE 1

The requirement to report to the Secretary if termination is not feasible would be eliminated for both covered entities and their contractors.

New requirements for business associate contracts

The proposed rule would make the following modifications to the requirements for business associate contracts:

- It would replace the current safeguard provision with a requirement that business associates "use appropriate safeguards and comply, where applicable, with subpart C of this part [i.e., the Security Rule], with respect to electronic protected information, to prevent use or disclosure of the information other than as provided for by its contract."
- It would add a requirement to report to the covered entity breaches of unsecured PHI as required by the data-breach reporting rule. This would not replace the current requirement in the Security Rule to report security incidents of which the business associate becomes aware.
- It would add a requirement for business associates to obtain written agreements with their subcontractors who create, receive, or maintain electronic PHI (EPHI) to comply with the Security Rule. For agents (as opposed to subcontractors), the business associate would need only to obtain an agreement (not necessarily written) to implement reasonable and appropriate measures to protect EPHI.
- It would add a requirement that the business associate comply with the requirements of the Privacy Rule to the extent that the business associate is to carry out a covered entity's obligation under the Privacy Rule (for example, providing individuals with access to health information or other rights).

It is worth noting that these modifications bear little resemblance to the kinds of contract amendment that have been circulating since the enactment of the HITECH Act.

Implementation of new contract requirements

The NPRM proposes a transition process to allow covered entities and business associates to continue to operate under existing contracts for up to one year and 240 days after the publication date of the final regulation, unless the agreement is renewed or modified sooner (although renewals or modifications made within the first 60 days after the effect date would not affect the grace period, and the extension of "evergreen" contracts would not be a renewal for this purpose). The transition period will only be available to contracts that complied with the prior requirements on the date of publication of the final rule.

Penalties

Under the HITECH Act, business associates that violate the Security Rule or the required terms of their business associate contracts are now subject to the same civil and criminal penalties as covered entities. To effect this provision, the NPRM proposes adding references to "business associate" to the civil money penalty provisions of the Rules. Further the NPRM proposes to add a provision providing for civil money penalty liability against a business associate for the acts of its agent.

Responsibility of covered entities for violations by business associates

The proposed rule would delete a provision of the Enforcement Rule that provides an exception to the liability of a covered entity for the acts of agents where the agent is a business associate, the relevant contract requirements have been met, the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and the covered entity did not fail to act as required by the Privacy or Security Rule with respect to such violations. There is a similar provision in the Privacy Rule that is not being deleted. The apparent effect is that a covered entity would be directly liable for the acts of business associates who are "agents" under common law; the "pattern or practice" rule would apply if the business associate was an independent contractor, and not an "agent." HHS has made this same troubling distinction in connection with last year's data breach reporting rule. In the commentary, HHS states:

> "We propose to remove this exception to principal liability for the covered entity so that the covered entity remains liable for the acts of its business associate agents, regardless of whether the covered entity has a compliant business associate agreement in place. This change is necessary to ensure, where the covered entity has contracted out a particular obligation under the HIPAA Rules, such as the requirement to provide individuals with a notice of privacy practices, that the covered entity remains liable for the failure of its business associate to perform that obligation on the covered entity's behalf. We do not believe this proposed change would place any undue burden on covered entities, since covered entities are customarily liable for the acts of their agents under agency common law.

BACK TO PAGE 1

"We note that this proposed regulatory change does not create liability for covered entities with respect to business associates that are not agents, e.g., independent contractors. The determination of whether a business associate is an agent of a covered entity, or whether a subcontractor is an agent of a business associate, will be based on the facts of the relationship, such as the level of control over the business associate's or subcontractor's conduct."

Privacy Rules

The HITECH Act modified the Privacy Rule in several respects. The proposed rule would implement these modifications, and make some others suggested by comments that HHS has received.

Requests for special restrictions

Under the HIPAA Privacy Rule, an individual may request special restrictions on the use or disclosure of his or her health information, but a covered entity is not required to accede to the request. Under the HITECH Act, a covered entity must comply with the requested restriction if the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment), and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

The proposed regulation would implement this new right. In the commentary, HHS says that a provider may not require a patient to pay out-of-pocket for all services in order to restrict disclosures of certain services. HHS also requests comment on what obligation providers should have to notify downstream providers of the restriction, and particularly how providers who use electronic prescribing could alert a pharmacy of the restriction, so that the pharmacy does not submit a claim to the health plan for drugs related to the restricted service.

Minimum necessary use and disclosure

The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit its uses and disclosures of PHI, and its requests for PHI, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Privacy Rule does not say what constitutes the minimum necessary PHI—this is left to the covered entity to establish by policies and procedures.

The HITECH Act will require covered entities to limit their uses, disclosures, and requests to the extent practicable, to a limited data set, or "if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request." The effect of this provision is not entirely clear; in the NPRM, HHS interprets it as meaning that, in applying the minimum necessary rule, covered entities should consider the feasibility of using the minimum data set, but are not required to do so.

The HITECH Act provides that the covered entity or business associate disclosing PHI must determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure. This appears to be a modification of the current rule, which permits a covered entity to rely on the requester's determination when disclosing protected health information to public officials, other covered entities, and professionals providing services to the covered entity. HHS does not address this apparent change.

The Act requires the Secretary to issue guidance on what constitutes "minimum necessary" for purposes of the HIPAA rule within 18 months after the date of the enactment of the Act. Once the Secretary's guidance becomes effective, the statutory restriction will expire. In the NPRM HHS seeks public comment regarding what aspects of the minimum necessary standard covered entities and business associates believe would be most helpful to have the Department address in the guidance and the types of questions entities may have about how to appropriately determine the minimum necessary for purposes of complying with the Privacy Rule.

Sale of protected health information

The HITECH Act generally prohibits a covered entity or business associate from directly or indirectly receiving remuneration in exchange for any PHI of an individual without a valid authorization from the individual that includes a specification of whether the PHI may be further exchanged for remuneration by the entity receiving the PHI.

This prohibition does not apply if the purpose of the exchange is:

- Public health activities;
- Research, as long as the price charged reflects the costs of preparation and transmittal of the data for such purpose;

BACK TO PAGE 1

- Treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent PHI from inappropriate access, use, or disclosure;
- The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity;
- Remuneration that is provided by a covered entity to a business associate for activities involving the exchange of PHI that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement;
- To provide an individual with a copy of the individual's PHI pursuant to a request by the individual; or
- Otherwise determined by the Secretary in regulations to be similarly necessary and appropriate as the exceptions expressly provided for.

The proposed rule would generally follow the statutory provisions, with some additions:

- It would require an authorization for the sale of PHI to disclose that the covered entity will be receiving remuneration for the disclosure.
- It would extend the treatment exception to include disclosures for payment, to clarify that disclosures of PHI to obtain payment do not constitute sale of the information. It would also clarify that permitted charges to the individual for an accounting of disclosures would not be considered sale of PHI.
- It would add two new exceptions, allowing a covered entity to receive payment for a disclosure required by law, and allowing a covered entity to charge a reasonable, cost-based fee to prepare and transmit health information for any purpose for which disclosure is permitted.

Access to electronic health records

The HIPAA Privacy Rule requires a covered entity to give individuals access to and copies of their health information contained in a designated record set. If the covered entity maintains information in an electronic health record, the HITECH Act gives individuals a right to obtain a copy of this information in an electronic format and, if the individual chooses, to direct the covered entity to transmit the copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific. Any fee that the covered entity may impose for providing such individual with a copy of this information (or a summary or explanation of such information) if the copy (or summary or explanation) is in an electronic form may not be greater than the entity's labor costs in responding to the request for the copy (or summary or explanation). The HITECH Act provides no guidance on how labor costs are to be determined.

The proposed regulation would extend this right to health information maintained electronically, whether or not in an electronic health record, properly speaking. It would also require the covered entity to provide the information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format agreed to by the covered entity and the individual. The rule would also include paper records under the individual's right to direct the covered entity to send the copy to a third party, but it would require the request to be signed by the individual. The rule would also allow a covered entity to charge for electronic media on which electronic records are provided, unless the individual supplies his or her own media, or requests transmission by e-mail.

Marketing

The HITECH Act clarifies that marketing communications are not health care operations, except those made (i) to describe a health-related product or service provided by, or included in a plan of benefits of, the covered entity making the communication, (ii) for treatment of the individual, or (iii) for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. This is consistent with the terms of the HIPAA Privacy Rule. However, the Privacy Rule permits a covered entity to receive remuneration for making these nonmarketing communications. The HITECH Act now prohibits financial remuneration, except where:

- The communication describes only a drug or biologic that is currently being prescribed for the individual, and any payment received by the covered entity in exchange for making a communication is "reasonable in amount," as defined by the Secretary in regulation, or

BACK TO PAGE 1

- The communication is made by a business associate on behalf of the covered entity; and (ii) the communication is consistent with the business associate contract between the business associate and covered entity.

Otherwise, a covered entity requires the individual's authorization to use PHI for marketing if it receives remuneration for doing so.

The proposed regulation would do the following:

- It would revise the exception for communications regarding treatment to distinguish more clearly between treatment (communications about which are not marketing and would not require authorization) and health care operations (communications about which are marketing and would require authorization if they encouraged the individual to buy something). Generally, population-based communications would be considered health care operations, requiring authorization; communications tailored to a particular individual's health care needs would be treatment-related, and would not require authorization (subject to the new notice and opt-out requirements discussed below if they are subsidized by a third party).

- It would add a definition of "financial remuneration," the receipt of which would take the communication out of the exceptions. The term would mean direct or indirect payment from a third party whose product or services are being marketed.

- For purposes of the exception for communications relating to drugs and biologics currently being prescribed for the individual, it would require that the payment be reasonably related to the covered entity's cost of making the communication.

Insofar as the HITECH Act appears to prohibit a provider from receiving remuneration from a third party to make treatment-related communications to a patient about the provider's products and services, HHS finds the Act ambiguous. HHS proposes to allow such communications, as long as the provider states in its notice of privacy practices that it intends to make such communications and to receive payment from a third party for making them, and the notice of privacy practices and the communication itself inform the individual that he or she may opt out of receiving such subsidized communications. HHS requests comments on the scope of the opt out —whether it should cover all future subsidized treatment communications, or just those concerning the particular product or service described in the current communication.

Fundraising

The Act requires the Secretary to provide by rule that any written fundraising communication shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communications to elect not to receive any further such communication. The Privacy Rule provides that if an individual opts out the covered entity must make reasonable efforts to ensure that individuals who opt out are not sent such communications. The Act provides that when an individual elects not to receive any further fundraising communications, the election will be treated as a revocation of authorization under the Privacy Rule.

HHS interprets this as a flat prohibition against sending fundraising communications to someone who has opted out, and the proposed rule would simply prohibit further fundraising communications to such a person. The rule would also require covered entities to include a statement of the individual's right to opt out in its notice of privacy practices.

In addition, the proposed rule would require an opt-out mechanism that does not require the individual to incur an undue burden or more than a nominal cost, such as an e-mail address or a toll-free telephone number. Requiring an individual to write and send a letter would not suffice. A covered entity would be precluded from conditioning treatment on an individual's agreeing to receive fundraising communications.

HHS solicits comments on two questions—one, whether an opt-out should apply to all future fundraising communications, or only to the current campaign; and two, whether the information that can be used for fundraising—currently limited to demographic information and dates of service—should be broadened to allow more targeted information, such as the department in which the individual received services.

Decedents

As a general rule the Privacy Rule protects the health information of decedents in the same way as that of the living. So, for example, information about deceased persons may be disclosed only to the individual's personal representative, but not to other family members or friends. The proposed rule would:

BACK TO PAGE 1

- Allow a covered entity to disclose PHI to a family member, or to friends involved in the person's care or payment for care, unless doing so is inconsistent with a prior expressed preference of the individual
- Remove all protection for records of persons deceased more than 50 years

Research authorizations

The Privacy Rule generally prohibits conditioning treatment on the individual's giving an authorization for use or disclosure of PHI. However, it allows a health care provider to condition participation in a clinical trial on the individual's providing an authorization for research. It also allows the combination of research authorizations with other written consents for the same study. However, it forbids combining a conditioned authorization (e.g., one for research), with an authorization that may not be conditioned. This sometimes results in multiple authorizations for clinical trials and related activities, such as tissue banking. The proposed rule would, therefore, allow a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities.

HHS also invites comments on whether to relax the rule that research authorizations be research-specific, so as to permit use of data or banked tissue for future research without the need to go back to the individual for an authorization, or to obtain a waiver from an institutional review board or a privacy board.

Immunization information

Under the current rules, a provider requires a formal authorization to provide health information about a student to his or her school. The proposed rule would permit a provider to disclose proof of immunization to a school, if the school is required by state law to obtain the information to admit the student, and the provider obtains the consent of the student's parent, guardian, or person acting *in loco parentis*. The consent may be informal, and may be oral.

Notice of privacy practices

The proposed rule would make several changes to covered entities' notices of privacy practices:

- If the covered entity intends to send subsidized treatment communications, its notice of privacy practices would be required to disclose this, and to notify the individual of the right to opt out.
- If the covered entity intends to send fundraising solicitations, the notice of privacy would now have to notify the individual of the right to opt out (the current requirement is just that notice of the opt-out right be included in the solicitation).
- The notice would be required to describe the need for an authorization for uses of psychotherapy notes, marketing, and sale of PHI for which authorization is required.
- The notice would be required to inform the individual that the covered entity may not refuse a request to withhold information from a health plan where the individual pays in full for the service.

Enforcement

The HITECH Act made substantial changes to the enforcement provisions of HIPAA. In October 2009 HHS issued an interim final Enforcement Rule to implement these changes (45 CFR § 160, Subpart D). This proposed rule would make changes to the Enforcement Rule necessitated by the other provisions of the proposed rule, and would clarify some terms.

First, the proposed rule would amend the Enforcement Rule to apply to business associates, since they are now covered directly by the security rule and certain other provisions of the HITECH Act.

Second, the proposed rule would implement provisions of the HITECH Act that require the Secretary to conduct a formal investigation of any compliant if a preliminary investigation indicates willful neglect. The rule would also provide that the Secretary will conduct a compliance review when a preliminary review of the facts indicates a possible violation due to willful neglect—in other words, a complaint is not necessary to trigger a formal investigation where the Secretary becomes aware of facts indicating willful neglect. The regulation would also permit the Secretary to conduct a compliance review in the absence of any complaint or apparent violation.

BACK TO PAGE 1

The HITECH Act requires the Secretary to impose a civil penalty for a violation due to willful neglect. The proposed regulation makes it clear that the Secretary will continue to pursue informal resolution of violations not due to willful neglect.

The HITECH Act established tiered penalties for violations of HIPAA and the HITECH Act. The lowest tier applies to violations of which the covered entity did not know, and, by exercising reasonable diligence, would not have known. The middle tier applies to a violation due to reasonable cause and not to willful neglect. The highest tier applies to violations due to willful neglect.

The proposed rule would amend the definition of "reasonable cause" to include knowing violations, as long as they do not indicate willful neglect. HHS gives the example of a covered entity that fails knowingly to respond in a timely manner to requests for access to information because of an unusually high volume of requests, but that catches up eventually. Another example is a covered entity that discloses information in good faith pursuant to a defective authorization.

The proposed rule would not change the meaning of "reasonable diligence" or "willful neglect," but the preamble gives some examples indicating how these terms would be interpreted.