



HEALTH LAW REPORTER



Reproduced with permission from BNA's Health Law Reporter, Vol. 19, No. 30, 07/29/2010. Copyright © 2010 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

HHS Proposed Rule Fine-Tunes HITECH and HIPAA Requirements



BY REECE HIRSCH

On July 14, 2010, the Department of Health and Human Services (“HHS”) published a notice of proposed rulemaking (the “Proposed Rule”) that would modify the HIPAA privacy, security and enforcement regulations (the “Privacy Rule,” “Security Rule” and “Enforcement Rule”).¹ The Proposed Rule primarily implements the provisions of the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), but it does contain a few features that have come as a surprise to many.

¹ “Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act,” 75 *Federal Register* 40868 (July 14, 2010).

Hirsch is a partner in the San Francisco office of Morgan, Lewis & Bockius LLP. He can be reached at rhirsch@morganlewis.com.

First, HHS takes this opportunity to clarify several provisions of the Privacy Rule that were not touched upon in the HITECH Act, but that have been a source of long-standing concern, such as the obligations of business associate subcontractors, research authorizations, and protections for decedents’ protected health information (“PHI”).

Second, HHS in some cases significantly has expanded upon the provisions of the HITECH Act. For example, HHS has placed additional restrictions on marketing communications for which a covered entity has received payment.

HHS states that the Proposed Rule does not address the following elements of the HITECH Act, which will be the subject of future rulemaking: (i) accounting for disclosures requirements and (ii) the penalty distribution methodology requirement, which will be based on recommendations to be developed by the U.S. Government Accountability Office (“GAO”). HHS also notes that it is not issuing regulations to address the new authority of state attorneys general to enforce HIPAA.

Unless otherwise indicated, the compliance date for all provisions of the Proposed Rule will be 180 days after the publication of the Final Rule.² HHS is accepting public comments on the Proposed Rule through Sept. 13, 2010. Throughout the Proposed Rule, HHS has raised a host of questions for public comment, some of which are highlighted in this article.

Business Associates

The HITECH Act imposed new privacy and security obligations on business associates and personal health record (“PHR”) companies. These new obligations were a corollary to the HITECH Act’s incentives promoting the adoption of electronic health records (“EHRs”). HHS seems to take the view that, in order to increase provider and consumer confidence in EHRs and PHRs, the companies that provide those products and aid in the electronic transmission of PHI must be subject to more direct privacy and security regulation.

Expansion of the Definition of Business Associate

The Proposed Rule would add the following to the definition of “business associate”:³

- “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”). This provision conforms HIPAA with the requirements of the PSQIA.
- Organizations that provide data transmission of PHI to a covered entity, such as Health Information Organizations and E-prescribing Gateways, and that require routine access to PHI. HHS reaffirms that “mere conduits” that do not access PHI, except on a random or infrequent basis, are not business associates.
- Vendors offering a PHR to one or more individuals on behalf of a covered entity.
- Subcontractors to a business associate that create, receive, maintain, or transmit PHI on behalf of a business associate.

The expansion of the definition of “business associate” to include subcontractors is one of the most significant new concepts introduced in the Proposed Rule, and was not addressed in the HITECH statute. HHS states that the intent of the provision was to ensure that privacy and security protections for PHI do not lapse simply because a function is performed by a “downstream entity” that has no direct contractual relationship with a covered entity.⁴ Subcontractors would be subject to Privacy Rule and Security Rule obligations to the same degree as a business associate, and would be directly liable for violations.

New Obligations of Business Associates

Prior to the HITECH Act, business associates were not directly regulated under HIPAA (unless the business associate also was a covered entity) and a violation of a business associate agreement merely subjected the business associate to potential contractual damages. The HITECH Act, and now the Proposed Rule, extends

new privacy and security obligations to business associates, who may now be directly subject to criminal and civil sanctions for violations of HIPAA.

The HIPAA Security Rule

The Proposed Rule would require business associates to comply with the Security Rule’s administrative, technical, and physical safeguard requirements and to implement security policies and procedures in the same manner as a covered entity.⁵ HHS clarifies in the Proposed Rule that business associates also must comply with 45 C.F.R. § 164.306, which states certain general rules governing Security Rule compliance, such as the factors that covered entities must take into account in deciding which security measures to use.⁶ It is now clear that HHS intends to apply the Security Rule to business associates in precisely the same way that it applies to covered entities. The Proposed Rule also inserts conforming references to the term “business associate” throughout the Security Rule.

Some subcontractors to business associates, which now are brought within the definition of “business associate” by the Proposed Rule, are likely to face challenges in meeting the new obligation to implement a full Security Rule compliance program. Prior to the Proposed Rule, it was sufficient for the subcontractor to make certain representations to the business associate that it had reasonable and appropriate safeguards in place.

The HIPAA Privacy Rule

In contrast to the approach taken with the Security Rule described above, the HITECH Act does not impose all of a covered entity’s Privacy Rule obligations upon business associates. Instead, business associates may be subject to HIPAA penalties if they violate the required terms of their business associate agreements.

The Proposed Rule implements this change by providing that a business associate may use or disclose PHI only in accordance with the mandated terms of its business associate agreement or as required by law. A business associate also may not use or disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity. However, a business associate still is permitted to engage in certain uses and disclosures of PHI for its own purposes, such as (i) data aggregation, (ii) management and administration of the business associate’s operations, and (iii) legal compliance.⁷ Any other use or disclosure of PHI by a business associate would violate both the terms of the business associate agreement and the Privacy Rule.

Business associates are *required* to disclose PHI:

- When required by the Secretary of HHS (the “Secretary”) to investigate or determine the business associate’s compliance with the Privacy and Security Rules; and
- To the covered entity, an individual or an individual’s designee, as necessary to respond to an individual’s request for an electronic copy of PHI.⁸

⁵ 75 Fed. Reg. at 40916 (to be codified at 45 C.F.R. § 164.104(b)).

⁶ 75 Fed. Reg. at 40917 (to be codified at 45 C.F.R. § 164.306).

⁷ 75 Fed. Reg. at 40920 (to be codified at 45 C.F.R. § 164.502(a)(4)).

⁸ 75 Fed. Reg. at 40919 (to be codified at 45 C.F.R. § 164.502(5)).

² 75 Fed. Reg. at 40913 (to be codified at 45 C.F.R. § 160.105).

³ 75 Fed. Reg. at 40912 (July 14, 2010) (to be codified at 45 C.F.R. § 160.103 (definition of “business associate”).

⁴ 75 Fed. Reg. at 40873.

Business associates also will be subject to the Privacy Rule's "minimum necessary" standard, and must make reasonable efforts to limit uses and disclosures of PHI, and PHI requested from a covered entity, to the minimum necessary to accomplish the intended purpose.⁹

Subcontractor Business Associate Agreements

Prior to the HITECH Act, business associates were required to "ensure" that a subcontractor "agree" to the same privacy and security obligations that apply to the business associate with respect to PHI.¹⁰ This provision often led business associates to enter into written agreements with subcontractors, but a written agreement was not expressly required. The Proposed Rule would require a business associate to enter into a written agreement with a subcontractor in order to obtain satisfactory assurances that the subcontractor will comply with applicable provisions of the Privacy and Security Rules.¹¹

HHS notes that the obligation to enter into a business associate agreement with a subcontractor rests solely with the business associate, and not the covered entity.¹² A covered entity is not required to enter into an agreement with a subcontractor of its business associate. The form of a subcontractor business associate agreement would be identical to the "upstream" business associate agreement and would contain all of the same required provisions.

If a business associate becomes aware of a pattern or practice of activity of a subcontractor that would constitute a material breach or violation of the subcontractor business associate contract, then the business associate must take reasonable steps to cure the breach or to terminate the contract, if feasible.¹³ Prior to the HITECH Act, a similar obligation has been imposed upon covered entities that become aware of violations or material breaches of a business associate contract by a business associate.¹⁴

The Proposed Rule eliminates a requirement that covered entities report to the Secretary when, despite a material breach or violation by the business associate, termination of the business associate contract is not feasible. Given that under the HITECH Act business associates are now directly liable for HIPAA violations, and both covered entities and business associates are required to report certain breaches of unsecured PHI to the Secretary, HHS deemed the requirement unnecessary.¹⁵

Amendment of Business Associate Agreements

The HITECH Act's provisions requiring amendment of business associate agreements have given rise to a considerable amount of uncertainty among covered entities and business associates. While the HITECH Act stated that certain new requirements would need to be incorporated into business associate agreements, it was

unclear what those amendments should look like and which provisions should be incorporated. Faced with an initial statutory compliance deadline of Feb. 18, 2010, many organizations already have commenced amending business associate agreements to comply with the HITECH Act. On March 15, 2010, HHS indicated in an announcement on its website that it would not enforce business associate contracting requirements pending further guidance in the Proposed Rule.

The Proposed Rule requires that the following new provisions be added to business associate contracts:

- The so-called "safeguards" provision should be replaced with a provision requiring that business associates "use appropriate safeguards and comply, where applicable, with [the Security Rule], with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract."
- Business associates must report to the covered entity any breach of unsecured PHI, as required by the HITECH security breach notification regulations. This requirement would be in addition to existing requirements that business associates report unauthorized uses and disclosures of PHI under the Privacy Rule and security incidents under the Security Rule.
- Business associates must enter into written agreements with subcontractors that create or receive PHI on behalf of the business associate imposing the same restrictions that apply to the business associate with respect to the PHI.
- Business associates must 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.¹⁶ For example, if a business associate is providing an individual with access to PHI, that access must be provided in accordance with Privacy Rule requirements.

It should be noted that many of the amendments that have been executed prior to the Proposed Rule, including those that sought to closely follow the wording of the HITECH statute, include numerous provisions that would not be required by the rule. In the commentary to the Proposed Rule, HHS announced that it will provide sample language for revising business associate contracts, adding that "[w]hile the language is generic and may not suit complex organizations with complex agreements, we believe that it will help small entities with their contract revisions and save them time and money in redrafting their contracts to conform to the new rules."¹⁷ HHS states that it expects to provide the revised sample language when the Final Rule is issued.¹⁸

Compliance Date for Business Associate Contract Amendments

The Proposed Rule creates a transition period for amending business associate contracts in order to "prevent rushed and hasty changes" to thousands of ongoing business associate agreements.¹⁹ The Proposed

⁹ 75 Fed. Reg. at 40919 (to be codified at 45 C.F.R. § 164.502(b)(1)).

¹⁰ 45 C.F.R. § 164.504(e)(2)(ii)(D).

¹¹ 75 Fed. Reg. at 40919 (to be codified at 45 C.F.R. § 164.502(e)(1)(iii)).

¹² 75 Fed. Reg. at 40873 and 40919 (to be codified at 45 C.F.R. § 164.504(e)(1)(i)).

¹³ 75 Fed. Reg. at 40919 (to be codified at 45 C.F.R. § 164.504(e)(1)(iii)).

¹⁴ 45 C.F.R. § 164.504(e)(1)(ii).

¹⁵ 75 Fed. Reg. at 40888.

¹⁶ 75 Fed. Reg. at 40919-20 (to be codified at 45 C.F.R. § 164.504(e)(2)).

¹⁷ 75 Fed. Reg. at 40910.

¹⁸ 75 Fed. Reg. at 40909.

¹⁹ 75 Fed. Reg. at 40888.

Rule provides that (i) if a business associate contract that is compliant with pre-HITECH business associate contracting requirements is entered into prior to the publication date of the Final Rule and (ii) the contract is not renewed or modified during that time period that is 60 days to 240 days after the publication of the Final Rule, then the contract will be deemed to be compliant until the earlier of (i) the date the contract is renewed or modified on or after the 240-day post-publication date or (ii) the date that is one year and 240 days after the publication date of the Final Rule.²⁰

In short, covered entities have a transition period for amending business associate contracts that may extend for as long as one year and eight months after the publication of the Final Rule. Business associate contracts that are renewed or modified within 60 days after publication of the Final Rule would qualify for the transition period. If a business associate contract is subject to automatic or “evergreen” renewal, such a renewal would not end the period of deemed compliance.²¹

Covered entities and businesses associates will need to re-evaluate their business associate contracting strategies in light of the Proposed Rule, weighing whether they wish to take full advantage of the contracting transition period, or whether business and liability considerations favor sooner amendment.

Penalties

The Proposed Rule amends the HIPAA regulations to provide that business associates that violate the Privacy or Security Rules may be directly liable for civil money penalties.²² Conforming references to “business associates” are added throughout the civil money penalty provisions. In addition, a business associate is liable, in accordance with the federal common law of agency, for violations based upon the acts or omissions of agents, including workforce members and subcontractors, acting within the scope of the agency.²³

Liability of Covered Entities for Violations by Business Associates

The Enforcement Rule currently provides an exception for covered entity liability for the acts of an agent when (i) the agent is a business associate, (ii) the relevant contract requirements have been met, (iii) the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and (iv) the covered entity did not fail to act as required by the Privacy or Security Rule with respect to the violations.²⁴ The Proposed Rule would eliminate this exception, making covered entities directly liable for the actions of business associates who are agents within the meaning of federal common law. For business associates who are “independent contractors” rather than “agents,” the “pattern or practice” rule described above still would apply. HHS made a similar distinction between agents and subcontractors in the HITECH security breach notification rule. This principle of liability is easy to state, but much harder to apply with certainty

to specific contractual relationships because it requires evaluating the degree of control that the covered entity exercises over the business associate’s conduct. HHS notes:

“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.”²⁵

It is important to note HHS’s comment that a covered entity’s liability for the violations of an agent business associate is not contingent upon the execution of a business associate contract.

The Privacy Rule

Marketing

HHS long has been concerned with situations in which third parties subsidize communications between covered entities and patients and steadily has increased regulation of this area under the Privacy Rule and the HITECH Act. Under the Proposed Rule, a communication by a covered entity about a product or service that encourages the recipient of the communication to purchase or use the product or service would not be a marketing communication if that communication is:

- for treatment by a health care provider (including for case management, care coordination, or to recommend alternative treatments, therapies, health care providers, or settings of care to the individual), provided that if the communication is in writing and the covered entity receives remuneration for making the communication, certain notice and opt-out requirements are met;
- to provide refill reminders or communicate about a drug or biologic currently prescribed to the individual, provided any remuneration received for making the communication is reasonably related to the cost of making the communication; or
- for the following health care operations purposes, unless the covered entity receives remuneration for making the communication: (i) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication; or (ii) for case management or care coordination, contacting individuals with information about treatment alternatives, and related functions, to the extent these activities do not fall within the definition of treatment.²⁶

The Proposed Rule imposes new limitations on communications made by covered entities that involve remuneration from third parties that were not found in the HITECH Act. In particular, the Proposed Rule im-

²⁰ 75 Fed. Reg. at 40924 (to be codified at 45 C.F.R. § 164.532).

²¹ 75 Fed. Reg. at 40890.

²² 75 Fed. Reg. at 40914 (to be codified at 45 C.F.R. § 160.402(a)).

²³ 75 Fed. Reg. at 40915 (to be codified at 45 C.F.R. § 160.402(c)(2)).

²⁴ 45 C.F.R. § 160.402(c).

²⁵ 75 Fed. Reg. at 40879.

²⁶ 75 Fed. Reg. at 40918 (to be codified at 45 C.F.R. § 164.501 (definition of “Marketing”)).

poses new restrictions on treatment communications for which the covered entity receives remuneration. While treatment communications remain excluded from the definition of “marketing” (and thus do not require individual authorization), a new notice and opt-out requirement is imposed when the treatment communications involve remuneration from a third party. This provision would necessitate changes to a covered entity’s notice of privacy practices, as discussed below.

With respect to the opt-out for treatment communications involving third-party remuneration, HHS encourages covered entities to consider use of a toll-free phone number, e-mail address, or other “simple, quick, and inexpensive” way for individuals to opt-out of receiving future communications. HHS notes that requiring the individual to mail a letter to the covered entity requesting the opt-out may constitute an “undue burden.”²⁷

The Proposed Rule also defines “financial remuneration” for purposes of the marketing rules as “direct or indirect payment from or on behalf of a third party whose product or service is being described.”²⁸ Direct or indirect payment does not include any payment for treatment of an individual.

HHS acknowledges that it may be difficult to determine in some cases whether a communication is for treatment or health care operations purposes. Therefore, HHS requests comment on the notice and opt-out requirements for treatment communications.²⁹ HHS also requests comment on whether an individual’s opt-out should cover all future subsidized treatment communications, or just communications regarding the specific products and services described in the communication.³⁰

Fund Raising

The HITECH Act required HHS to issue a rule that requires all written fund-raising communications from a covered entity provide the recipient with an opportunity to opt out of any future fund-raising communications. Implementing this requirement, the Proposed Rule provides:

- each fund-raising communication must include a clear and conspicuous opportunity for the individual to elect not to receive further fund-raising communications (once again, the individual should not incur an undue burden or more than a nominal cost, and HHS prefers a toll-free phone number, e-mail address, or similar method);
- treatment or payment cannot be conditioned on an individual’s choice to receive fund-raising communications;
- fund-raising communications may not be sent to someone who has opted out of such communications; and
- a covered entity must include a statement in its notice of privacy practices that the entity may use and disclose PHI for fund raising but that individuals have the right to opt out of receiving such communications.³¹

²⁷ 75 Fed. Reg. at 40886.

²⁸ 75 Fed. Reg. at 40919 (to be codified at 45 C.F.R. § 164.501 (definition of “Marketing”).

²⁹ 75 Fed. Reg. at 40886.

³⁰ 75 Fed. Reg. at 40886.

³¹ 75 Fed. Reg. at 40922 (to be codified at 45 C.F.R. § 164.514(f)(1)(ii)).

The Privacy Rule had required that a covered entity make reasonable efforts to ensure that individuals who opt out do not receive further communications. In keeping with the HITECH Act’s provisions, the Proposed Rule toughens that standard by simply making any further fund-raising communications with a person who has opted out a violation of the Privacy Rule. This provision is intended to effectuate the intent of the HITECH Act’s provision requiring that fund-raising opt out operate like a revocation of authorization.³²

HHS solicits comment regarding whether a fund-raising opt out should apply only to the current campaign or to all future fund-raising communications. HHS also seeks comment on several other fund-raising issues, including the Privacy Rule’s current requirement limiting the information that a covered entity may use for fund-raising communications to demographic information and dates that health care services were provided, and whether the department of service or similar information also should be available for use.³³

Sale of PHI

The HITECH Act generally prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of PHI unless the covered entity has obtained an authorization from the individual that states whether the PHI can be further exchanged for remuneration by the entity receiving the information. This prohibition on the sale of PHI becomes effective six months after HHS issues final implementing regulations on the subject.

The Proposed Rule implements the HITECH Act provision, providing that the prohibition does not apply if the purpose of the exchange is:

- public health activities;
- research, so long as the payment is a “reasonable, cost-based fee” reflecting the costs of preparing and transmitting the PHI for such purpose;
- treatment of the individual;
- the sale, 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; or
- to provide an individual with a copy of the individual’s PHI pursuant to a request by the individual.³⁴

The Proposed Rule adds the following new provisions to those set forth in the HITECH Act:

- the treatment exception would be expanded to include disclosures for payment, clarifying that disclosures of PHI to obtain payment are not sales of PHI;
- an authorization for the sale of PHI would be required to state that the covered entity will be receiving remuneration for the disclosure;

³² 75 Fed. Reg. at 40897.

³³ 75 Fed. Reg. at 40897.

³⁴ 75 Fed. Reg. at 40921 (to be codified at 45 C.F.R. § 164.508(a)(4)).

- the prohibition does not apply to a reasonable, cost-based fee charged to the individual by a covered entity for an accounting of disclosures;
- covered entities are allowed to receive payment for a disclosure that is required by law; and
- the sale of PHI is permitted as determined by the Secretary pursuant to regulations to be necessary and appropriate, so long as the fee charged is either reasonable and cost-based or expressly permitted by another law.³⁵ HHS notes that this provision would permit a covered entity to disclose PHI in compliance with any state law that places a limit on the fees a health care provider can charge to prepare, copy, and transmit medical records.³⁶

Requests for Restrictions on Disclosures of PHI

The Privacy Rule currently provides individuals with a right to request a restriction on a covered entity's use or disclosure of PHI for treatment, payment, or health care operations purposes, but covered entities are not required to grant such requests. The HITECH Act created an exception to this rule, providing that a covered entity must comply with a requested restriction if the disclosure is (i) to a health plan for purposes of carrying out payment or health care operations (and not for treatment), (ii) not otherwise required by law, and (iii) 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 Rule implements this new HITECH Act requirement³⁷ and HHS offers clarifying comments. HHS states that a provider may not require a patient to pay out-of-pocket for all services in order to restrict disclosures with respect to certain services.³⁸ HHS also notes that under most HMO plans an individual does not have the option of paying the provider in full for treatment or service received. Therefore, HMO enrollees might have to use an out-of-network provider in order to ensure that certain PHI is not disclosed to their HMO.³⁹

HHS requests comments on whether a provider should have an obligation to inform other "downstream" health care providers of such a restriction. In particular, HHS questions how a provider using an e-prescribing tool could alert the pharmacy to a restriction requested by an individual and ensure that the prescription claim is not disclosed to the health plan.⁴⁰

Access to Electronic PHI

The Privacy Rule gives individuals the right to obtain copies of their PHI from a covered entity, to the extent the information is maintained in a designated record set. The HITECH Act expanded those access rights with respect to PHI maintained in an electronic health record ("EHR"), allowing the individual to obtain a copy of the information in an electronic format and direct the covered entity to transmit the copy directly to a person or entity designated by the individual, so long as the choice is clear, conspicuous, and specific.

³⁵ 75 Fed. Reg. at 40921 (to be codified at 45 C.F.R. § 164.508(a)(4)).

³⁶ 75 Fed. Reg. at 40892.

³⁷ 75 Fed. Reg. at 40923 (to be codified at 45 C.F.R. § 164.522(a)(1)(vi)).

³⁸ 75 Fed. Reg. at 40899.

³⁹ 75 Fed. Reg. at 40900.

⁴⁰ 75 Fed. Reg. at 40900.

In the commentary to the Proposed Rule, HHS notes that granting these access rights with respect to EHRs, but not other electronic PHI maintained in designated record sets, would result in a complex set of disparate requirements for access to electronic PHI.⁴¹ Therefore, in the Proposed Rule, HHS extends the HITECH Act's access right to all PHI maintained electronically by a covered entity. Covered entities would be required to provide the information in the electronic form and format requested by the individual, if it is readily producible or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.⁴²

The Proposed Rule also would allow a covered entity to charge for electronic media on which electronic records are provided, unless the individual supplies the media or requests transmission by e-mail.⁴³ The HITECH Act provided that any fee charged by the covered entity for providing access to EHR data may not be greater than its labor costs in responding to the request. HHS invites comment on the types of activities related to managing electronic access requests that should be compensable aspects of labor.⁴⁴

The Proposed Rule also would grant the individual a new right to direct the covered entity to send a paper copy of PHI to a third party; the HITECH Act only had extended that right to electronic PHI in an EHR.⁴⁵

Notice of Privacy Practices

The Proposed Rule would mandate the following changes to a covered entity's notice of privacy practices:

- If the covered entity intends to send subsidized treatment communications, its notice of privacy practices would be required to disclose that fact and to notify the individual of the right to opt out.
- If the covered entity intends to send fund-raising solicitations, the notice of privacy practices would have to notify the individual of the right to opt out (in contrast to the current Privacy Rule requirement to simply include notice of the opt-out right in the solicitation).
- The notice would be required to describe the need for an authorization for uses of psychotherapy notes, marketing, and the 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 out-of-pocket in full for the service.⁴⁶

HHS views these proposed modifications as material changes to the notice, requiring covered entities to promptly revise and distribute their notices. HHS recognizes that this may be burdensome for health plans, which are required to provide revised notices to enrollees within 60 days of any material revision. HHS is

⁴¹ 75 Fed. Reg. at 40901.

⁴² 75 Fed. Reg. at 40923 (to be codified at 45 C.F.R. § 164.524(c)(2)(i)).

⁴³ 75 Fed. Reg. at 40923 (to be codified at 45 C.F.R. § 164.524(c)(4)(ii)).

⁴⁴ 75 Fed. Reg. at 40902.

⁴⁵ 75 Fed. Reg. at 40923 (to be codified at 45 C.F.R. § 164.524(c)(3)(ii)).

⁴⁶ 75 Fed. Reg. at 40923 (to be codified at 45 C.F.R. § 164.520(b)(1)(ii)(E)).

seeking comment on several options with respect to these health plan notifications.⁴⁷

The Minimum Necessary Rule

The Privacy Rule requires covered entities to limit uses and disclosures of, and requests for, PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The HITECH Act provides that a covered entity shall be treated as being in compliance with the minimum necessary rule only if the covered entity limits the PHI used or disclosed, to the extent practicable, to the limited data set or, if needed by the covered entity, to the minimum necessary.

The HITECH Act requires HHS to issue guidance on the minimum necessary rule within 18 months after the date of enactment of the Act. When the HHS guidance becomes effective, the HITECH Act's statutory restriction will expire. HHS solicits comment on (i) which aspects of the minimum necessary standard should be addressed in the guidance and (ii) how to appropriately determine the minimum necessary for purposes of Privacy Rule compliance.⁴⁸ In the Proposed Rule, HHS elects not to propose any regulatory modifications with respect to the minimum necessary rule because the subject will be addressed in the upcoming guidance.⁴⁹

Decedents

The Privacy Rule has required that covered entities protect the privacy of a decedent's PHI to the same extent as the PHI of a living individual. Therefore, when an authorization is required for disclosure of PHI, a covered entity may disclose a decedent's PHI only after obtaining a written authorization from the decedent's personal representative, which can have the effect of limiting disclosures to family and friends. HHS also notes that concerns have been raised regarding the difficulty of locating a personal representative to authorize disclosure of PHI, particularly after the decedent's estate has closed.⁵⁰

The Proposed Rule would:

- allow a covered entity to disclose PHI to a family member, other relative, or a close personal friend of the decedent, or to friends involved in the decedent's care or payment for care, unless doing so is inconsistent with a prior expressed preference of the decedent,⁵¹ and
- remove all privacy protections for records of persons deceased for more than 50 years.⁵²

Research Authorizations

The Privacy Rule generally prohibits covered entities from conditioning treatment on the provision of an authorization. However, a covered entity is permitted to condition the provision of research-related treatment on obtaining the individual's authorization, such as for a clinical trial (a "conditioned authorization"). The Privacy Rule also generally prohibits compound authoriza-

tions in which two authorizations are combined in one document.

HHS expressed concern that recruitment for clinical research trials has been hampered, in part, due to the numerous forms that must be signed to participate in clinical trials and related activities, such as tissue banking and specimen collection for a central repository.⁵³ To address this concern, the Proposed Rule would permit 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 to opt in to the unconditioned research activities.⁵⁴

HHS also seeks comment on whether to modify the rule that authorizations for research purposes must be research-study specific. If the rule were to be relaxed, a research authorization also might permit use of PHI in a research database or tissue bank without the need to obtain a separate authorization from the individuals, or a waiver from an institutional review board or privacy board.⁵⁵

Student Immunization Records

Although the subject was not addressed in the HITECH Act, HHS responded in the Proposed Rule to concerns that the Privacy Rule has made it more difficult for parents to provide, and for schools to obtain, necessary immunization documentation for students. Most states have "school entry laws" that prohibit a child from attending school unless the school has proof that the child has been appropriately immunized.

In response to these concerns, the Proposed Rule would permit covered entities to disclose proof of immunization to schools in states that have school entry or similar laws. While authorization no longer would be required for such disclosures, the covered entity still would be required to obtain an agreement, which may be oral, from a parent, guardian, or other person acting for the individual, or directly from the individual if he or she is an emancipated minor.⁵⁶ HHS is seeking comments as to whether covered entities should be required to document such an oral agreement in writing.⁵⁷

Enforcement

The HITECH Act introduced a variety of new measures aimed at strengthening HIPAA enforcement efforts, including increased civil penalties. The Enforcement Rule issued by HHS in October 2009 sought to implement the HITECH Act's changes. The Proposed Rule makes additional modifications to the Enforcement Rule and clarifies certain key terms.

The Proposed Rule adds references to business associates throughout the Enforcement Rule to implement the HITECH Act's provisions imposing direct liability on business associates for violations of the HITECH Act and the HIPAA Privacy and Security Rules.

The Enforcement Rule currently provides that HHS may investigate privacy complaints or conduct compli-

⁴⁷ 75 Fed. Reg. at 40898.

⁴⁸ 75 Fed. Reg. at 40896.

⁴⁹ 75 Fed. Reg. at 40896.

⁵⁰ 75 Fed. Reg. at 40894.

⁵¹ 75 Fed. Reg. at 40921 (to be codified at 45 C.F.R. § 164.510(b)).

⁵² 75 Fed. Reg. at 40919 (to be codified at 45 C.F.R. § 164.502(f)).

⁵³ 75 Fed. Reg. at 40893.

⁵⁴ 75 Fed. Reg. at 40921 (to be codified at 45 C.F.R. § 164.508(b)(3)(i) and (iii)).

⁵⁵ 75 Fed. Reg. at 40894.

⁵⁶ 75 Fed. Reg. at 40922 (to be codified at 45 C.F.R. § 164.512(b)(1)(vi)).

⁵⁷ 75 Fed. Reg. at 40895.

ance reviews. In accordance with the HITECH Act, the Proposed Rule provides that HHS *will* investigate complaints or conduct compliance reviews when a review of the facts indicates a potential violation due to willful neglect.⁵⁸ The Proposed Rule also requires HHS to conduct a compliance review when a preliminary review of the facts indicates a possible violation due to willful neglect, meaning that HHS may initiate a compliance review even in the absence of a complaint when it becomes aware of facts indicating willful neglect.⁵⁹ The Proposed Rule also provides that HHS no longer is required to resolve cases of noncompliance due to willful neglect by informal means, such as demonstrated compliance or a corrective action plan.⁶⁰ HHS retains the ability to resolve cases not involving willful neglect through informal means.

The Proposed Rule makes clear that HHS may disclose PHI if permitted under the federal Privacy Act.⁶¹ The proposed change is necessary to permit the Secretary to cooperate with other law enforcement agencies, such as state attorneys general pursuing HIPAA actions on behalf of state residents or the Federal Trade Commission pursuing remedies under other consumer protection authorities.⁶²

The HITECH Act's tiered penalty structure is based upon the following degrees of culpability: (i) violations of which the person did not know (and by exercising reasonable due diligence would not have known), (ii) violations due to reasonable cause and not to willful neglect, and (iii) violations due to willful neglect. The Proposed Rule modifies the definition of reasonable cause

in order to clarify the demarcations between the categories of culpability.

The Proposed Rule would modify the definition of "reasonable cause" as follows: "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect."⁶³ This revised definition adds the "knowledge," "reasonable diligence," and "willful neglect" standards.

HHS applies the new definition of reasonable cause in an example. A covered entity receives an individual's request for access, but does not respond within the required time period. HHS's investigation reveals that the covered entity had appropriate access policies and procedures in place, but had received an unusually high volume of requests. Most access requests were responded to within the required time period, but a few were not. In this case, the covered entity had knowledge of the violations, but circumstances made it unreasonable for the covered entity to fully comply with the access requirements, despite the exercise of ordinary business care and prudence. The covered entity also lacked the conscious intent or reckless indifference associated with willful neglect.⁶⁴

For consistency with the HITECH Act's tiered penalty structure, the Proposed Rule also would modify the Enforcement Rule to explicitly state that HHS must consider "the nature and extent of the violation" and "the nature and extent of the harm resulting from the violation" in determining a civil money penalty amount. The Proposed Rule also includes a new reference to reputational harm as a cognizable form of harm to be considered in penalty determinations.⁶⁵

⁵⁸ 75 Fed. Reg. at 40913 (to be codified at 45 C.F.R. § 160.306(c)(1)).

⁵⁹ 75 Fed. Reg. at 40914 (to be codified at 45 C.F.R. § 160.308(a)).

⁶⁰ 75 Fed. Reg. at 40877, 40914 (to be codified at 45 C.F.R. § 160.312(a)(1)).

⁶¹ 75 Fed. Reg. at 40914 (to be codified at 45 C.F.R. § 160.310(c)(3)).

⁶² 75 Fed. Reg. at 40876.

⁶³ 75 Fed. Reg. at 40914 (to be codified at 45 C.F.R. § 160.401 (definition of "Reasonable cause")).

⁶⁴ 75 Fed. Reg. at 40878.

⁶⁵ 75 Fed. Reg. at 40915 (to be codified at 45 C.F.R. § 160.408(a) and (b)).