Bulletin

INCompliance

July 2010

New HIPAA-HITECH Proposed Regulations Issued

On Thursday July 14, 2010, the Department of Health and Human Services (HHS) published proposed regulations in the Federal Register on many provisions of the HI-TECH Act that would modify the Privacy Rule, Security Rule, and Enforcement Rule of the Health Insurance Portability and Accountability Act (HIPAA).

General Changes

Conforming Changes. Many of the revisions in the proposed regulations would serve to update existing HIPAA rules to conform to the HI-TECH Act. Most notably, because the HI-TECH Act makes business associates subject to certain privacy, security, and enforcement rules, many of the proposed changes would add language to clarify this issue. For example, 45 CFR 160.202 would be revised to clarify that certain definitions that currently only refer to covered entities are applicable to business associates. These changes are not described in further detail in this Client Bulletin.

Effective Date. The regulations would provide that most provisions become effective 180 days after the final regulations are published. HHS also proposed to add a new provision to 45 CFR 160.105 that would codify the 180-day compliance date generally for implementation of new or modified standards in the HIPAA rules.

Preemption (45 CFR 160.201). In addition to making minor changes to the provisions of HIPAA regarding the preemption of state law, the proposed regulations would add language to clarify that HIPAA does not create a federal evidentiary privilege and that neither the HIPAA statute nor regulations give effect to state physician-patient privilege laws in federal court proceedings.

Changes Regarding Business Associates

Subcontractors of Business Associates (45 CFR 160.501, 45 CFR 164.504(e)). Perhaps the most radical change in the proposed regulations would revise the definition of "business associate" to include subcontractors of business associates who receive Protected Health Information (PHI). Thus, subcontractors of business associates would themselves be business associates. This is a significant expansion of the business associate concept. Currently, business associates are required to ensure that subcontractors receiving PHI agree "to the same restrictions and conditions that apply to the business associate with respect to the [PHI];" however, subcontractors are not considered business associates. Under the proposed regulations, subcontractors of business associates, as business associates themselves, would be subject to (1) civil and criminal penalties and direct enforcement activities, (2) the breach and notice of breach rules, and (3) the sections of the Security Rule applicable to business associates.

The proposed regulations would require business associates to obtain satisfactory assurances from each subcontractor that receives PHI that the subcontractor will safeguard the PHI received. The satisfactory assurances would be required to be documented through a written contract that meets the applicable requirements of a business associate contract under 45 CFR 164.504(e). That is, business associates must have

business associate contracts with all subcontractors that receive PHI from the business associate. The proposed regulations would also provide that business associates have the same requirements as covered entities with respect to business associates' subcontractors. This subsection mirrors covered entity requirements regarding business associate agreements and, thus, if a business associate is aware of noncompliance by its subcontractor, the business associate would be required to respond in the same manner that a covered entity must respond when it is aware of noncompliance of a business associate (i.e., take reasonable steps to cure the breach, or end the violation and if that cannot be done, then terminate the contract).

Business Associate Contracts (45 CFR 164.504(e)). The proposed regulations would remove the requirement that a covered entity must report to HHS if termination of the contract was not feasible because the business associate now has direct liability for violations of HIPAA and the breach provisions allow the secretary to receive notice of breaches. Subsections (e)(2)(ii)(B)-(D) would be modified to reflect the obligations imposed on business associates by the HI-TECH Act. A new subsection (e)(2)(ii)(H) would be added to state that when a business associate is carrying out the obligations of a covered entity, the business associate must comply with the requirements of the Privacy Rule that would apply to the covered entity.

Transition Provisions for Business Associate Contracts (45 CFR 164.532). The proposed regulations would add a new section to ease the administrative burden to covered entities and business associates from the required modifications of their business associates contracts. If the covered entity or the business associate has an existing business associate contract that complies with the prior provisions of the HIPAA rules and such contract is not renewed or modified prior to the compliance date of the final regulations, then this provision would allow the covered entity or the business associate to continue to operate under that business associate contract for up to one year beyond the compliance date without amending their business associate contract.

New business associate contracts entered into after the effective date of the final regulations or existing business associate contracts that are modified or renewed after the effective date of the final regulations will need to be brought into compliance with all new requirements. Despite the language regarding "renewals," however, note that the commentary explains that "evergreen" contracts with automatic renewals are not deemed to be renewed for this purpose; that is, the contract qualifies for the full transition period even if there is an automatic renewal after the effective date of the final regulations. It is notable that this would only apply to written arrangements and not oral arrangements. Note also that the grandfathering of existing business associate contracts would only affect the requirement to modify the form of the business associate contract; the business associate would still be required to meet all of the applicable HIPAA rules upon the effective date of the rules.

Lack of Business Associate Agreement. The commentary in the rule also states that HHS is clarifying that a person "is a business associate if it meets the definition of 'business associate,' even if a covered entity … fails to enter into the required contract with the business associate."

Uses and Disclosures of PHI (45 CFR 164.502). The proposed regulations would add a new subsection to provide specific permitted uses and disclosures of PHI by business associates and required disclosures by business associates. The new subsection would reiterate that a business associate is permitted to use or disclose PHI only as permitted or required by its business associate agreement or as required by law (as provided in the HI-TECH Act). Also, the new subsection would provide that a business associate is required to disclose PHI to (1) HHS when required to investigate or determine the business associate's compliance with HIPAA and (2) the covered entity, the individual, or individual's designee as necessary to satisfy a covered entity's obligations with respect to a request for a copy of electronic PHI.

Minimum Necessary Requirement (45 CFR 164.502(b)). The proposed regulations would clarify that the minimum necessary requirement applies to business associates as well as covered entities.

Workforce (45 CFR 160.103). The proposed regulations would revise the definition of "workforce" to clarify that the definition applies to business associates. That is, the employees, volunteers, trainees, and other persons whose conduct is under the direct control of the business associate are members of the business associate's workforce.

Security Rule: General Rules (45 CFR 164.306). The proposed regulations would make the general rules section of the Security Rule, 45 CFR 164.306, applicable to business associates. The HI-TECH Act made four sections of the Security Rule (45 CFR 164.308, 164.310, 164.312, and 164.316) applicable to business associates but did not include 45 CFR 164.306. 45 CFR 164.306 contains general rules regarding many of the Security Rule provisions, including those applicable to business associates. Thus, HHS states that it believes it necessary to make the general rules in 45 CFR 164.306 also applicable to business associates.

Security Rule: Organizational Requirements (45 CFR 164.314). The proposed regulations would make the organizational requirements of the Security Rule, 45 CFR 164.314, applicable to business associates. This section was also not one of the four sections of the Security Rule made applicable to business associates by the HI-TECH Act. However, because 45 CFR 164.308 (which is applicable to business associates) requires compliance with 45 CFR 164.314, HHS states that it believes it necessary to make the organizational requirements in 45 CFR 164.314 also applicable to business associates. The proposed regulations would also revise the provisions regarding business associate contract requirements in 45 CFR 164.314 to reflect that a business associate contract is required between a business associate and a subcontractor that receives PHI and that such contract must meet all of the same requirements as those between covered entities and business associates (as discussed above).

PSQIA Activities (45 CFR 160.103). The proposed regulations would revise the definition of "business associate" to add patient safety activities to the list of functions and activities a person may undertake on behalf of a covered entity that give rise to a business associate relationship. Thus, Patient Safety Organizations (PSOs) under the PSQIA would be treated as business associates, except that a component PSO within a health care provider would not be a business associate, but would be a workforce members of the covered entity. Health Information Organizations, E-Prescribing Gateways, and Other Persons Facilitating Data Transmission. As required by the HI-TECH Act, the proposed regulations would revise the definition of "business associate" to include entities such as Health Information Exchanges, E-prescribing Gateways, and Regional Health Information Organizations that provide data transmission of PHI and require access to the PHI.

Changes To The Privacy Rule

Marketing (45 CFR 164.501). The proposed regulations would substantially rewrite the definition of "marketing" to (1) distinguish the exceptions for treatment communications from those communications made for health care operations; (2) add a definition of financial remuneration; (3) provide that health care operations for which financial remuneration is received are considered to be marketing and require an authorization; (4) provide that written treatment communications for which financial remuneration is received are subject to certain notice and opt out conditions; and (5) provide a new limited exception from the remuneration prohibition for refill reminders.

"Financial remuneration" would be defined to mean direct or indirect payment from or on behalf of a third party whose product or service is being described. The financial remuneration must specifically be in exchange for making the communication and be from or on behalf of the entity whose product or service is being described.

Treatment communications (including communications for case management, care coordination, or to direct or recommend alternate treatments, therapies, health care providers or settings of care to the individual) would be expressly excluded from the definition of marketing; provided, however, that if financial remuneration is received in exchange for making the treatment communication, then these "subsidized treatment communications" would require certain notice and opt out conditions. Thus, HHS is not proposing to require an authorization for subsidized treatment communications about health-related products or services so long as the covered entity includes a statement in its Notice of Privacy Practices that it intends to send such subsidized treatment communications to an individual and the covered entity gives the individual the opportunity to opt out of receiving such communications. This opt out provision must be a simple, quick, and inexpensive way to opt out such as an 800 telephone number or an email address. HHS indicates that it would be an undue burden to require the individual to send a letter.

An authorization is required for any subsidized health care operations communication. Because of the disparate treatment between a subsidized treatment communication and a subsidized health care operations

communication, covered entities must be diligent in determining whether the communication is a treatment communication or a health care operation communication. HHS requests comments on these differences and on the alternative of excluding subsidized treatment communications altogether or the alternative of requiring authorizations for all subsidized communications whether they are for treatment or health care operations.

The proposed regulations would include an exception for communications regarding refill reminders as long as the financial remuneration is reasonably related to the covered entity's cost of making the communication. HHS requests comments on the scope of this exception (specifically, whether the communication about drugs must be related to the drugs currently being prescribed or whether communications regarding generic alternatives or new formulations should fall within the exception). HHS is also requesting comments on the types and amounts of costs that should be allowed under this provision.

Sale of PHI (45 CFR 164.508(a)(4)). The proposed regulations would add a new provision to make the sale of PHI a specific circumstance for when an authorization is required if it is in exchange for direct or indirect remuneration. To ensure that individuals can make informed decisions about whether to authorize such disclosure, the authorization must state that the disclosure will result in remuneration to the covered entity. This new provision incorporates some, but not all, of the existing exceptions to authorization requirements in HIPAA. The new provisions would include an exception to clarify that authorization is not required when the disclosure is (1) otherwise permitted by HIPAA and the exchange of remuneration is merely "a reasonable, cost-based fee to cover the cost to prepare and transmit" the PHI or (2) to a business associate and the only remuneration is the payment for the performance of the business associate's activities. In addition, HHS notes that the new regulations would mean that if the recipient of PHI was a covered entity or business associate that the covered entity or business associate could not re-disclose that PHI in exchange for remuneration unless a valid authorization was obtained by that covered entity or business associate. HHS is specifically requesting comments on this "re-disclosure" provision.

Research (45 CFR 164.508(b)). The proposed regulations would amend this section to allow covered entities to combine conditioned and unconditioned authorizations for research studies provided that the authorization clearly differentiates between the conditioned and unconditioned research components and allows the individual the option to opt in to the unconditioned research activities. HHS notes that, given its interpretation that any authorization for research must be study-specific and must include a description of each purpose of the requested use and disclosure of PHI, concerns have been expressed that this encumbers secondary research and limits an individual's ability to agree to the use and disclosure for future research purposes. HHS is considering a number of options in the area of future research and specifically requests comments on the following:

- Whether the Privacy Rule should permit an authorization for uses and disclosures of PHI for future research purposes to the extent such purposes are adequately described in the authorization such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for future research.
- Whether the Privacy Rule should permit an authorization for future research only to the extent the description of the future research included certain elements or statements specified by the Privacy Rule and, if so, what those elements should be.
- Whether the Privacy Rule should permit the option under the first bullet as a general rule but require certain disclosure statements on the authorization in cases where the future research may encompass certain types of sensitive research activities (i.e., genetic analysis or mental health research).

Fundraising (45 CFR 164.514(f)). The HI-TECH Act requires HHS to provide by rule that a covered entity must provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications. The proposed regulations would fulfill this requirement, but also would make a number of other changes to the existing fundraising rule, including:

- Requiring that the method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than nominal cost and notes that requiring an individual to send a letter by mail to opt out of fundraising would constitute an undue burden;
- Providing that a covered entity may not condition treatment or payment on an individual's choice with respect to receiving fundraising communications; and

- Providing that a covered entity may not send fundraising communications to an individual who has elected not to receive such communications (consistent with the HI-TECH Act statutory language already in effect).

Interestingly, HHS is also seeking public comment on whether it should revise the fundraising rule to allow covered entities to use or disclose information related to the patient's department of service for fundraising activities without patient authorization. This request for comment is in response to feedback HHS has received from covered entities, arguing that the prohibition on the use or disclosure of such information harms their ability to raise funds from patients.

Notice of Privacy Practices for Protected Health Information (45 CFR 164.520). The proposed regulations would require covered entities to include a statement in their Notice of Privacy Practices regarding the types of uses and disclosures of PHI that require authorization of the individual (including disclosures of psychotherapy notes and disclosures for purposes of marketing). Further, the Notice of Privacy Practices would also have to include a statement that other uses and disclosures not described in the Notice of Privacy Practices will be made only with the individual's authorization.

The proposed regulations would also require new Notice of Privacy Practices provisions for covered entities that either: (1) send treatment communications to individuals concerning treatment alternatives or other health-related products or services where the covered entity receives financial remuneration in exchange for making the communication or (2) contact individuals to raise funds for the entity. In both instances, the covered entities must inform patients of these practices and of the patients' right to opt out of such communications.

Right to Request Restriction of Uses and Disclosures (45 CFR 164.522(a)). The HI-TECH Act requires covered entities to agree to requests for restrictions on uses and disclosures of PHI if the request is (1) on disclosures of PHI to a health plan for the purpose of carrying out payment or health care operations and (2) only applicable to PHI that pertains solely to a health care item or service which has been paid out-of-pocket in full. The proposed regulation would clarify that, as long as the covered entity is paid for the services by the individual or another person on behalf of the individual other than the health plan, the covered entity would be required to abide by the restriction. HHS also emphasizes that, if an individual's out-of-pocket payment is not honored (e.g., a bounced check), the covered entity may then submit the PHI to the health plan for payment as the individual did not fulfill the requirements necessary to obtain a restriction.

Access of Individuals to Protected Health Information (45 CFR 164.524). The HI-TECH Act strengthened the Privacy Rule's right of access with respect to covered entities that use or maintain an electronic health record by giving individuals the right to (1) obtain from the covered entity a copy of such information in an electronic format and (2) direct the covered entity to transmit such copy directly to the individual's designee for a fee not greater than the covered entity's labor costs. HHS has determined that limiting this expanded right of access to information contained in electronic health records "could result in a complex set of disparate requirements for access to protected health information in electronic health records systems versus other types of electronic records systems." Accordingly, the proposed regulations would require any covered entity that electronically maintains PHI about an individual, in one or more designated record sets, to provide the individual with an electronic copy of such information (or summary thereof if agreed to by the individual) in the electronic form and format requested or in an otherwise agreed upon form and format.

The proposed regulations would also require a covered entity to transmit a copy of PHI directly to another person designated by the individual if the individual's request is in writing, signed by the individual and clearly identifies the designated person and where to send the copy of PHI. While the HI-TECH Act included language to this effect with regard to PHI contained in electronic health records, the proposed regulations would apply this rule without regard to whether the PHI is in electronic or paper form.

Disclosure of Student Immunizations to Schools (45 CFR 164.512(b)). In its description of the proposed regulations, HHS notes that it has heard concerns that the Privacy Rule may make it more difficult for parents to provide, and for schools to obtain, the necessary immunization documentation for students, which may prevent students' admittance into the schools. Accordingly, the proposed regulation would permit covered entities to disclose proof of immunization to schools in states that have school entry or similar laws. Written authorization

would no longer be required for such disclosures, but the covered entity would instead be required to obtain agreement, which could be oral, from the parent, guardian, or the individual, if the individual is an adult or emancipated minor. PHI of Deceased Individuals (45 CFR 160.103). The proposed regulations would revise the definition of "protection health information" to provide that the HIPAA Privacy and Security Rule do not apply to PHI of persons who have been deceased for more than 50 years. Definition of Health Care Operations. (45 CFR 164.501). The definition would be expanded to specifically include the patient safety activities as defined in the PSQIA implementing regulations.

Minimum Necessary Requirement (45 CFR 164.514(d)). The HI-TECH Act requires HHS to issue guidance on what constitutes "minimum necessary" within eighteen (18) months of enactment. Such guidance has not yet been issued. HHS requests "public comment on what aspects of the minimum necessary standard covered entities and business associates believe would be most helpful to have HHS 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."

Changes to the Enforcement Rule

Compliance and Investigations (45 CFR 160.310). The proposed regulations would modify existing HIPAA regulations that provide PHI obtained by HHS will not be disclosed except for enforcing HIPAA and as required by law. The proposed revision would permit HHS to disclose PHI to other government agencies for civil or criminal law enforcement as permitted under the federal Privacy Act (5 USC 552a(b)(7)). This change would permit HHS to share PHI with states' attorneys general to facilitate their new HIPAA enforcement authority.

Imposition of Civil Monetary Penalties (45 CFR 160.401). The proposed regulation would clarify the "state of mind" aspect of the second category of culpability associated with the four tiers of civil monetary penalty amounts created by the HI-TECH Act. Civil monetary penalties for HIPAA violations increase based on which category it falls into (1) when the covered entity or business associate did not know of the violation and would not have known by exercising reasonable diligence; (2) when the violation was due to reasonable cause but was not due to willful neglect; (3) when the violation was due to willful neglect but the covered entity corrected the violation within 30 days of discovery of the violation; and (4) when the violation was due to willful neglect but the covered entity failed to correct the violation within 30 days of discovery. The first, third and fourth categories all depend on "state of mind," but the current definition of "reasonable cause" in the second category does not. The rule revises the definition of "reasonable cause" to clarify that it applies when a violation of HIPAA occurs and the covered entity or business associate knew or by exercising reasonable due diligence would have known of the violation, but in which there was not willful neglect. That is, the definition clarifies application to all circumstances between category one (no knowledge of the incident) and when the covered entity or business associate acted with willful neglect.

Basis for Civil Monetary Penalties (45 CFR 160.402). Currently, a covered entity is not liable for the acts of a business associate if there is a compliant business associate agreement in place, the covered entity did not know of the violation and the covered entity did not fail to act as required by HIPAA with respect to the violation. The proposed regulation would eliminate this exception when the business associate is acting as an agent of the covered entity. The exception would remain in place when the business associate is merely a contractor of the covered entity. The issue of whether a business associate is an "agent" of the covered entity, thus, would become much more significant as a covered entity would always be liable for the HIPAA violations of a business associate who is an "agent."

Factors Considered in Determining Amount of Civil Monetary Penalties (45 CFR 160.408). The proposed regulations would amend the structure and list of factors considered by HHS in determining the amount of civil monetary penalties assessed for HIPAA violations. Specifically, "the nature and extent of the violation" would remain as a factor but would now include consideration of "the number of individuals affected." Also, "the nature and extent of the harm resulting from the violation" would remain as a factor (as amended by the HI-TECH Act) but would now include "reputational harm" in addition to physical or financial harm. Finally, the current factor or "prior violations" would be revised to "indications of noncompliance" to make the concept more broadly inclusive of past noncompliance and not limited only to past formal findings of violations.