A Timely Analysis of Legal Developments

ASAP®

In This Issue:

July 2010

Close analysis of the Department of Health and Human Services' voluminous proposed revisions to the HIPAA regulations reveals that, if adopted, employers would need to revise several key HIPAA documents.

What Do Employers with HIPAA-Covered Health Plans Really Need to Know About Recently Proposed Revisions to HIPAA Regulations?

By Philip L. Gordon

The U.S. Department of Health and Human Services (HHS) published on July 14, 2010, a voluminous Notice of Proposed Rulemaking (NPRM), containing dozens of proposed amendments to three sets of Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations: the Privacy Rule; the Security Rule; and the Enforcement Rule. The proposed amendments are directed principally at implementing the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which amended HIPAA and went into effect on February 17, 2010. A careful review of the NPRM for its impact on employers who sponsor HIPAA-covered plans reveals that, if the proposed changes were adopted, employers would be required to revise their business associate agreements, their HIPAA notice of privacy practices, and their policies for responding to access requests. The NPRM also provides employers with a roadmap for avoiding civil monetary penalties.[1]

Employers should note that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies only to a narrow subset of employee health information, i.e., individually identifiable health information created or received by, or on behalf of, a group health, dental, vision, or pharmacy benefit plan, employee assistance program, health care reimbursement flexible spending account, or certain long-term care plans. This information must relate to the past, present, or future physical or mental health condition of the plan participant, treatment for the condition, or payment for the treatment and is referred to in HIPAA parlance as protected health information (PHI).

Amending Business Associate Agreements

Under the HIPAA Privacy Rule, a covered health plan is prohibited from disclosing PHI to a "business associate," a service provider that creates or receives PHI on the plan's behalf (e.g., a third-party administrator, pharmacy benefits manager, or insurance broker) unless the plan enters into a written agreement, known as a "business associate agreement," which contains provisions prescribed by the Privacy

Rule. The HITECH Act created uncertainty about the content of these business associate agreements because several provisions of the Act create new obligations for business associates, but the Act does not itself specify which, if any, of those obligations must be addressed in the business associate agreement. As a result, since the HITECH Act went into effect on February 17, 2010, service providers have inundated employers subject to HIPAA with proposed amendments to business associate agreements which contain a bewildering array of contract language.

The proposed regulations should eliminate the confusion by revising the Privacy Rule's provision that describes the required content of a business associate agreement. Surprisingly, the proposed regulations, if adopted, would require employers to make only limited changes to their existing business associate agreements. These changes would require that language addressing the following points be added to existing business associate agreements: (a) the business associate must comply with the HIPAA Security Rule; (b) the business associate must report breaches of unsecured PHI to the covered entity; (c) the business associate's subcontractors must agree to the same restrictions on the use and disclosure of PHI as the business associate; and (d) if the business associate performs any of the covered entity's compliance obligations (such as distributing the notice of privacy practices), the business associate must comply with the HIPAA Privacy Rule to the same extent as the covered entity with respect to those delegated obligations.

Notably, many business associate agreements amended in the rush to meet the HITECH Act's February 17, 2010 compliance date already address the first three required changes. Consequently, if the proposed regulations are adopted, many employers likely would be required to make only a single addition to their recently amended business associate agreements to address point (d), above. As discussed below, employers would have plenty of time before having to make that one revision.

Timing for Amending Business Associate Agreements

The proposed regulations would grandfather all existing business associate agreements until *eighteen months* after the proposed rules become final, which likely will take an additional six to twelve months given that HHS has solicited public comment on several of the proposed amendments.

Extending Business Associate Agreements to Subcontractors

One major new development is that the proposed regulations, if adopted, would classify subcontractors of business associates as business associates whereas, under current regulations, only the service provider directly under contract with the covered health plan is classified as a business associate. As a result of this proposed change, first-tier business associates would be required to enter into business associate agreements with their subcontractors. These agreements would be required to contain the same provisions as the business associate agreements between the covered health plan and its business associate. If the first-tier business associate becomes aware of a pattern of activity by the subcontractor that constitutes a material breach of the agreement, then the first-tier business associate must ensure that the subcontractor cures the breach or the first-tier business associate must terminate the contract. In addition, the first-tier business associate is liable for the subcontractor's HIPAA violations if the subcontractor is acting as the business associate's agent within the meaning of federal common law.

Importantly, this change does *not* impose any new requirements on covered health plans. The proposed regulations specifically provide that the covered entity is *not* required to enter into a business associate agreement with subcontractors of its business associates, and the covered entity is *not* liable for the subcontractor's violations of HIPAA.

However, under any business associate agreement between a first-tier business associate and its subcontractor, the subcontractor would be required to report any security breach that it discovers directly to the covered entity. Consequently, an employer should consider including in its agreement with its first-tier business associate a provision that: (a) identifies the person (by job title) whom the business associate must contact in the event of a security breach; and (b) requires the business associate to provide that contact information to its subcontractors.

Avoiding Civil Monetary Penalties

The proposed regulations create a roadmap for employers seeking to avoid civil monetary penalties for HIPAA violations. Under the proposed rules, HHS is required to investigate any complaint that, upon preliminary review, suggests the covered entity's alleged HIPAA violation resulted from "willful neglect." In addition, HHS *must* impose a monetary penalty if the agency finds willful neglect, albeit the penalty would be lower if the covered entity corrected the violation within thirty days of receiving notice from HHS. Willful neglect means "conscious, intentional failure or reckless indifference to the obligation to comply with the regulation that is the target of the complaint." By contrast, the proposed regulations *bar* HHS from imposing a penalty if the covered entity demonstrates that the violation did not result from willful neglect and was promptly corrected after the covered entity knew, or should have known, of the violation.

An employer can best avoid a finding of willful neglect — and, therefore, a civil monetary penalty — by establishing HIPAA policies and procedures in compliance with the regulations, by making good faith efforts to implement them, and by training employees authorized to access PHI. In addition, whenever an employer receives notice of an alleged violation from HHS, the employer should cooperate with HHS and promptly correct the violation.

Revising The Notice of Privacy Practices

The Privacy Rules requires that covered health plans distribute a notice of privacy practices to plan participants and prescribes the content of that notice. The proposed regulations would require two minor revisions to the existing notice.

First, the notice would be required to state expressly that the covered health plan, except in limited circumstances, must obtain a plan participant's written authorization to: (a) use or disclose psychotherapy notes; (b) use or disclose PHI for marketing purposes; or (c) receive remuneration for the disclosure of PHI. Second, the notice must inform plan participants of a new right conferred on them by the HITECH Act. That right permits plan participants to instruct health care providers not to disclose to the health plan any PHI related to services for which the plan participant pays out-of-pocket.

Recognizing the potentially high cost and undue burden to employers of having to distribute a revised notice of privacy practices to all plan participants, HHS has solicited comments on whether employers could communicate these changes by some means other than issuing a revised notice. HHS also has solicited comments on whether covered entities should be required to revise their notice of privacy practices to inform individuals of their right to receive notice in the event of a security breach. Given these outstanding issues, it would be premature for employers to revise their notice of privacy practices before HHS issues final regulations.

Establishing Procedures for Plan Participants to Exercise Their Right to Access PHI in Electronic Form

The Privacy Rule confers on plan participants the right to request access to their PHI and implicitly assumes that the covered entity will respond to that request with documents in paper form. The proposed regulations add new requirements for responding to an individual's request to access PHI in electronic form.

Under those proposed revisions, the employer generally must produce PHI in the requested electronic form. The employer also must comply with the plan participant's request to transmit PHI in electronic form to a third party. The employer can require that the plan participant: (a) make the request in a signed writing; and (b) clearly identify the recipient of the PHI and how to deliver the PHI to the recipient. The employer also can request reimbursement for any electronic media, such as a CD or flash drive, that it must provide to comply with the plan participant's request.

Employers typically rely upon a third-party administrator to respond to access requests. Consequently, as a practical matter, these changes will have limited impact on employers. However, employers are required to have written policies on how to respond to

access requests. If the proposed regulations are adopted, those policies would need to be revised to address the new requirements for requests to access PHI in electronic form.

Conclusion

While the Notice of Proposed Rulemaking is voluminous and the proposed changes numerous, the revisions that would affect employers with HIPAA-covered plans are relatively few and the burden of addressing them should not be substantial. At the same time, the proposed regulations' strict handling of HIPAA violations involving willful neglect means that these changes could not be ignored. Organizations can submit comments on or before September 13, 2010, to: U.S. Department of Health and Human Services, Office for Civil Rights, Attention: HITECH Privacy and Security Rule Modifications, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201 or through www.regulations.gov/search/Regs/home.html#home.

Philip L. Gordon is a Shareholder in Littler Mendelson's Denver office and the Chair of Littler's Privacy and Data Protection Practice Group. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, or Mr. Gordon at pgordon@littler.com.

---

[1] This ASAP does not address proposed changes that do not have a significant impact on employers, such as changes to the regulations governing the use of protected health information for fundraising or marketing or prohibiting the sale of such information.