Thomas D. Bixby
Law Office LLC
Legal Advice for Health Plans

HEALTH LAW ALERT
January 21, 2013

"Omnibus" Privacy Rule Issued

HHS Imposes More Stringent Breach Notification Standard
Requires Changes to Privacy Notices, Business Associate Agreements

On Thursday, the Department of Health and Human Services (HHS) published a final rule, adopting a variety of changes to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules. The amended rules adopt changes required by the HITECH Act and the Genetic Information Nondiscrimination Act ("GINA"), as well as making some policy changes, incorporating previously-furnished guidance into the rules, and correcting errors in previously-issued rules.

Many of the amendments, such as making business associates (including subcontractors) directly subject to the Privacy and Security Rules and prohibiting the sale of protected health information, are the direct result of the HITECH Act and GINA. As these statutes have been in effect for several years, the amendments are unlikely to require significant changes in how health plans do business. Other amendments, however, will require health plans to make such changes. Chief among these is HHS's amendment to the Breach Notification Rule, which requires a presumption that notice is required for every breach, allowing a covered entity (or business associate) to overcome the presumption only if there is a "low probability" that information has been compromised.

The changes go into effect on September 23, 2013. The final rule will be formally published in the Federal Register on Friday, January 25. (I will also publish my compilation of the HIPAA Administrative Simplification Rules incorporating the new standards as well as other related material on the 25th (click here to see the Resources page of my website).

Breach Notification

For the past three years, HHS has viewed a non-permitted use or disclosure of protected health information as a "breach" for which notice is required only if the use or disclosure "poses a significant risk of harm to the [affected] individual." HHS concluded that "some persons may have interpreted [this] risk of harm standard . . . as setting a much higher threshold for breach notification than we intended to set." As a result, HHS made three changes to the standard for determining whether notice of a breach is required. First, the amended rule requires a presumption that notice is required for any breach. Although this presumption may be overcome, the amended rules will make concluding no breach is required more difficult than the current standard. The second change is that the threshold will be revised from "a significant risk" to "a low probability" of risk.

HHS's third change to the Breach Notification standard is to replace the determination of whether the breach causes "harm to the individual" with a determination of whether the information has been "compromised." Specifically, the amended rule requires covered entities (and business associates) to determine whether "there is a low probability that the protected health information has been compromised." Covered entities (and business associates) make this determination by conducting a risk assessment, which must take into account (at least) four factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to protected health information has been mitigated.

HHS asserts that the focus of this new standard on determining whether protected health information has been "compromised" is more "objective" than the "harm to the affected individual" standard. Yet, the examples HHS provides in the preamble to the final rule and the four factors HHS requires to be used in the risk assessment (see above) incorporate many of the same "harm to the individual" considerations as the original rule.

For example, HHS suggests that a misdirected fax to a covered entity would involve a lower probability that information was "compromised" than a misdirected fax to another person (see factor (ii) above). Similarly, HHS indicates that some diagnoses, treatment plans, or medical tests are more sensitive than others and therefore make the probability of protected health information being "compromised" more likely (see factor (i) above). In each case, these considerations are applied in essentially the same manner as they are in making the "harm to the affected individual" determination.

HHS promises more guidance on how to determine whether information has been "compromised." But for now, the change does not appear to make the process substantially more "objective."

Business Associates and Subcontractors Subject to Privacy & Security Rules

Provisions of the amended rules that arise out of the HITECH Act require business associates to comply with the Privacy and Security Rules. The amended rules define the term "business associate" to include "subcontractors." While covered entities are not required to directly engage these "subcontractors" in "business associate agreements," a business associate that hires a subcontractor must engage the subcontractor in a written agreement that meets the same requirements as a covered entity's agreement with its business associate.

Privacy Practices Notice

Content. HHS will require (at least)[1] three additions to the privacy practices notices that health plans must provide to members. First, a health plan will be required to explain in its privacy practices notice that an authorization is necessary to allow a health plan to (a) use or disclose protected health information for "marketing" and (b) sell protected health information.[2] A health plan must also add to its notice an explanation that an individual will receive notification of a breach of the individual's unsecured protected health information. Finally, a health plan that engages in "underwriting"—see box below—must include in its privacy practices notice a statement that it is prohibited from using or disclosing genetic information for that purpose.

Publication. Health plans that do not already have these terms in their privacy practices notices must re-publish the notices with the additional provisions. Health plans that post their privacy practices notice on their website have a different publication deadline for hardcopy notices than health plans that do not post their notices:

- Health plans that post notices on their website must prominently post a revised notice on their website by the effective date of the material change to their notice (in this case, September 23) and provide a hardcopy of the revised notice (or information about the changes to the notice) in the "next annual mailing to individuals then covered by the plan."
- Health plans that do **not** post notices on their websites must provide a hardcopy of the revised notice (or information about the changes to the notice) within 60 days of the effective date of the material change to their notice (September 23).

Business Associate Agreements

The amended rules revise the requirements for terms of "business associate agreements." Many health plans

GINA Provisions

The amended rules prohibit the use and disclosure of genetic information for "underwriting" purposes. GINA-related terms, including the term "underwriting," generally have the same meaning as in the GINA Rules that HHS, the Department of Labor, and the IRS published in 2009. (Click here for my Health Law Alert on the subject.)

This means that the prohibition on use and disclosure of genetic information extends to determining eligibility for benefits under a health plan, as well as the more traditional meaning of "underwriting."

[1] Privacy notice changes that are unlikely to affect most health plans are also addressed in the amended rule, such as changes relating to fundraising practices.

[2] A health plan that maintains "psychotherapy notes" will also be required to include in its privacy practices notice a statement that most uses or disclosures of psychotherapy notes may be made only with an authorization. Health plans that do not maintain this type of information are not required to include this statement in their notices, however.

have already included some of these new requirements in their business associate agreements since the HITECH Act went into effect three years ago.

First, the agreement must require the business associate to comply with the Security Rule with respect to any electronic protected health information it creates for or receives from or on behalf of the health plan. Second, the agreement must require the business associate to report any "breach" of protected health information for which notification is required under the Breach Notification Rule.

Finally, when a business associate is to carry out an obligation of the covered entity under the HIPAA Rules, the agreement must require the business associate to "comply with the requirements of [the HIPAA Rules] that apply to the covered entity in the performance of such obligation." Thus, for example, HHS explains that this provision would apply when a third party administrator is contractually obligated "to distribute a health plan's privacy practices notice to participants on a timely basis." If the third party administrator fails to distribute the notices in compliance with the Privacy Rule's requirements, "the third party administrator would not be directly liable under the HIPAA Rules" because the Privacy Rule imposes the obligation on the covered entity, not its business associate. Nevertheless, the third party administrator "would be contractually liable, for the failure." This provision would also apply, for example, to business associates obligated by contract to conduct standard transactions in compliance with the HIPAA Transactions Rule.

Health plans (with respect to business associates) and business associates (with respect to subcontractors) are **not** required to incorporate these provisions into business associate agreements that are in effect prior to January 25, 2013 (the date the amended rules will be formally published), until the earlier of:

- The date on which the agreements are renewed or modified; or
- September 22, 2014.

Business associate agreements that are entered into on or after January 25, 2013 must contain these terms by the effective date of the amended rules—September 23, 2013.

Other Information Concerning Amended Rules

"Access accounting": On May 31, 2011, HHS published a proposed rule addressing an individual's rights to disclosure accounting. One proposal HHS made was to allow an individual to obtain a report providing information about each time the individual's electronic protected health information is **accessed** in a designated record set. HHS does not address this proposal in the amended rules, leaving it to "be the subject of a future rulemaking."

Security Rule: HHS made no substantive changes to the Security Rule, other than to require that business associates comply with the Rule.

Prohibition on Sale of Protected Health Information: The amended rules implement the HITECH Act's prohibition on the sale of protected health information, including limited exceptions.

Prohibition on Payment for "Marketing" Communications: Similarly, the amended rules implement the HITECH Act's prohibition on conducting communications that the Privacy Rule's marketing provisions would otherwise permit if the covered entity (or business associate) sending the communications receives payment, directly or indirectly, for making the communications. (Limited exceptions apply.) Thus, for example, HHS explains that "an authorization would be required prior to a [health care provider] making a communication to its patients regarding the acquisition of . . . new state-of-the-art medical equipment if the equipment manufacturer paid the covered entity to send the communication."

* * * * * * * * * *

Please contact Tom Bixby at (608) 661-4310 or TBixby@tbixbylaw.com for more information.

Thomas D. Bixby Law Office LLC
(608) 661-4310 | www.tbixbylaw.com