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

HEALTH LAW ALERT
August 24, 2009

HHS Publishes Interim Final Data Breach Rule
Compliance Required in September, But Enforcement Delayed Until February

Today, the Department of Health and Human Services (HHS) published interim final rules that dictate notice requirements for HIPAA covered entities and their business associates that experience a breach of "unsecured protected health information." HHS drafted the rule to implement provisions of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), which was signed into law by President Obama in February as part of the American Recovery and Reinvestment Act of 2009. The rule is sandwiched between the HIPAA Security Rule and the HIPAA Privacy Rule, as a new Subpart D of Part 164 of the Code of Federal Regulations Title 45 (the "Data Breach Rule"). *See* 74 *Federal Register* 42739 (Aug. 24, 2009).

The Rule goes into effect on September 23, 2009, but HHS will "use [its] enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before . . . February 22, 2010." This delay is to reflect HHS's recognition "that it will take covered entities and business associates time to implement the processes and procedures necessary to comply with [the Data Breach Rule]" and HHS's concern that, prior to next February, its authority to impose sanctions for violations is not clear.

Generally, the Data Breach Rule addresses breaches of "unsecured protected health information"—protected health information that is not encrypted or destroyed. Under the Rule, a covered entity must notify each affected individual, HHS, and, in some cases, the media, of any breach that either the covered entity or its business associate experiences. A business associate, in turn, must notify the covered entity it serves of any breach the business associate experiences.

HHS Requests Comments on Rule; Due by October 23

HHS requests comments on the Interim Final Rule by October 23. HHS specifically requested comments on (i) federal preemption of State law (see side bar on page 2, below), (ii) a safe-harbor in the Data Breach Rule for limited data sets that do not contain zip codes or birth dates (*see* side bar on page 4, below), and (iii) HHS's economic analysis, including the costs and benefits of the Rule.

Although covered entities and business associates will not have to provide notice of "breaches" that do not "pose a significant risk of financial, reputational, or other harm," each time a covered entity or business associate relies on this exception it must perform a

risk assessment of the "breach" to determine whether it creates a "significant risk." The covered entity or business associate must document its risk assessment and maintain the documentation for six years.

The Data Breach Rule is written to "harmonize" with the Federal Trade Commission's ("FTC's") data breach rule, which affects vendors of personal health records and related entities. (Click here for information on the FTC Rule, *see* "Health Law Alerts"). Indeed, HHS stresses that it "consulted closely with the FTC in the development of these regulations" and that in rare cases in which a breach is subject to both rules, "the FTC will deem compliance with [the HHS Data Breach Rule] as compliance with FTC's rule."

Preemption of State Breach Notification Laws

The HIPAA Administrative Simplification standard for preemption of State laws applies to the Data Breach Rule. Hence, State laws that are "contrary" to the Data Breach Rule are preempted.

A State law is "contrary" to the Data Breach Rule (1) if "a covered entity would find it impossible to comply with both State and federal requirements" or (2) if the "provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of" the Data Breach Rule.

Under this standard, however, the Data Breach Rule is not likely to preempt many provisions of State law. As HHS explains, "in general we believe that covered entities can comply with both the applicable State laws and [the Data Breach Rule]. In addition, . . . we believe that, in most cases, a single notification can satisfy the notification requirements under State laws and this regulation."

Breaches for Which Notice is Required

Covered entities and their business associates have the burden of proving "that all notifications were made as required by [the Data Breach Rule]." As HHS explains, this means that "when a covered entity or business associate knows of an impermissible use or disclosure of protected health information, it should maintain documentation that all required notifications were made, or, alternatively," the reason (or reasons) notification is not required under the Data Breach Rule.

The first step in documenting compliance is determining when a "breach" occurs. Identifying a breach that is subject to the Data Breach Rule involves a four step analysis, explained in more detail, below. First, the Data Breach Rule applies to "breaches" of "unsecured protected health information." Second, a breach must involve a violation of the Privacy Rule. Third, a breach must "compromise the security or privacy of the protected health information." Finally, the Data Breach Rule excludes from the definition of "breach" three "situations Congress clearly intended to not constitute breaches."

Breach of Unsecured Protected Health Information. The Data Breach Rule applies only to "protected health information," as defined in the HIPAA Rules (*see* 45 C.F.R. § 160.103). HHS points out that "protected health information" includes information "in

any form or medium, including electronic, paper, or oral form." Breaches include, therefore, incidents involving protected health information on paper or communicated orally, as well as breaches involving electronic protected health information. But, no breach can occur with respect to data that is de-identified pursuant to Privacy Rule standards.

Only protected health information that is "unsecured" may be subject of a breach for purposes of the Data Breach Rule. Information is unsecured unless it is "rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by [HHS]." HHS currently specifies only two such technologies or methodologies: encryption and destruction. For details on appropriate encryption and destruction technologies and methodologies, *see* 74 *Federal Register* 19006 (April 27, 2009) as modified by Section II of 74 *Federal Register* 42739, 42741-43 (Aug. 24, 2009).

Breach Violates Privacy Rule. The Data Breach Rule dictates that a breach is "the acquisition, access, use, or disclosure of protected health information in a manner not permitted by [the Privacy Rule]." Thus, uses and disclosures that the Privacy Rule permits cannot be "breaches" for which a covered entity or business associate is required to give notice. HHS emphasizes that even an "incidental disclosure" permitted by the Privacy Rule,[1] such as a person who is not authorized to access protected health information overhearing a customer service representative's discussion of a specific claim, does not qualify as a breach. On the other hand, a violation of a covered entity's minimum necessary protocols could qualify as a breach.

Breach Compromises Security or Privacy. The Data Breach Rule includes a "harm threshold," such that a covered entity or business associate is not required to provide notice of uses or disclosures that cause minimal or no harm, even if they violate the Privacy Rule. Specifically, an impermissible use or disclosure does not qualify as a breach for notification purposes, unless the use or disclosure "poses a significant risk of financial, reputational, or other harm to the [affected] individual."

HHS explains that, to apply this standard, a covered entity or business associate must "perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure." A separate, fact-specific risk assessment must be performed to determine whether each potential breach meets the "harm threshold." HHS instructs that a person undertaking a risk assessment "should keep in mind that many forms of health information, not just information about sexually transmitted diseases or mental health, should be considered sensitive for purposes of the risk of reputational harm—especially in light of fears about employment discrimination."

[1] The Privacy Rule permits a covered entity to make a use or disclosure that is "[i]ncident to a use or disclosure otherwise permitted or required by [the Privacy Rule]," provided that the covered entity has in place appropriate safeguards to limit incidental disclosures and the otherwise-permitted use or disclosure complies with the Privacy Rule's minimum necessary limitation.

HHS stresses that "covered entities and business associates must document their risk assessments, so they can demonstrate, if necessary, that no breach notification was required following an impermissible use or disclosure of protected health information." This breach documentation must be maintained for six years.

Factors that the risk assessment may take into account include:

- **Who impermissibly used or received the protected health information.** Information impermissibly received by another covered entity or "a Federal agency that is obliged to comply with the Privacy Act" may involve less risk of harm, whereas "the risk of harm is much greater" with respect to information impermissibly disclosed to a third party "that does not have similar obligations to maintain the privacy and security of the information."

- **Steps to mitigate an impermissible use or disclosure.** When a covered entity takes "steps [that] eliminate or reduce the risk of harm to the individual to a less than 'significant risk,' then . . . the security and privacy of the information has not been compromised and, therefore, no breach has occurred." HHS suggests that "obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed" could qualify as an appropriate step.

- **The type and amount of protected health information.** HHS explains that "if the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach." Thus, disclosure of an individual's name and the fact that s/he received care at a hospital "may not constitute a significant risk of financial or reputational

Limited Data Sets

HHS recognized that "it would be impractical to require [notification of] individuals of a breach of information within a limited data set because, by definition, [a limited data set] excludes the very identifiers that would enable [entities] to identify the affected individuals and comply with the breach notification requirements." HHS also expressed concern that the Data Breach Rule not have a "chilling effect on the research and public health communities," which make extensive use of limited data sets.

To address these concerns, HHS provided a safe harbor for limited data sets that do not contain birth dates or zip codes. Under the Data Breach Rule, "breaches" involving such limited data sets do not meet the harm threshold necessary to trigger an obligation to provide notice of the breach.

Furthermore, HHS provided guidance with respect to application of the Data Breach Rule to "breaches" of information in limited data sets. First, HHS explained that, depending on the specific circumstances, a covered entity's or business associate's risk assessment could demonstrate that impermissible access to information in a limited data set did not meet the "harm threshold," meaning no breach notice would be required. Second, HHS explained that a covered entity is not responsible for limited data set breaches that occur after the limited data set has been given to a researcher or public health entity.

harm" and would not, therefore, qualify as a breach. This would not be the case, however, if the facility from which the individual received care was specialized—for example, an oncology or substance abuse facility.

HHS provides one "harm threshold" safe harbor for which no risk assessment is required. A covered entity or business associate that experiences an impermissible use or disclosure of information in a "limited data set" may determine that no breach occurred for which notice is required, provided that the limited data set did not contain dates of birth or zip codes. (For more information on how the Data Breach Rule applies to limited data set breaches, see the side bar on the previous page.)

Exceptions to Definition of "Breach." The Data Breach Rule includes three exceptions to the definition of breach based on provisions of the HITECH Act. Any impermissible use or disclosure of protected health information that qualifies under one of these exceptions is not a "breach" for purposes of determining whether notification is required. HHS emphasizes that a covered entity or business associate relying on one of these exceptions has the burden of proof "for showing why breach notification was not required." The exceptions are:

1. **Unintentional Use by Member of Workforce.** Impermissible use of or access to protected health information by a workforce member (or other person acting under the authority of the covered entity or business associate) is not a breach, provided that (i) the access or use was unintentional, in good faith, and within the scope of the workforce member's authority and (ii) the impermissible access or use does not result in further use or disclosure not permitted by the Privacy Rule.

2. **Inadvertent Disclosures to Authorized Persons.** Inadvertent "disclosures"[2] by one person authorized to access protected health information to another person authorized to access protected health information at the same covered entity or business associate are not "breaches" for which notice is required. This exception also applies to inadvertent disclosures by an authorized person at one covered entity that participates in an "organized health care arrangement" to an authorized person at another covered entity that participates in the same organized health care arrangement. In either case, the exception applies as long as the information is not subsequently used or disclosed in a manner that violates the Privacy Rule.

   HHS illustrates these first two exceptions by explaining no breach occurs when one member of a covered entity's workforce accesses an e-mail containing protected health information that another member of the covered entity's workforce accidently sent to him/her, provided that the recipient (i) is authorized

[2] The HIPAA Administrative Simplification Rules define "disclosure" to mean "divulging in any . . . manner information *outside the entity holding the information*." 45 C.F.R. § 160.103 ("disclosure") (emphasis added). This provision of the Data Breach Rule nevertheless uses the term "disclosure" to describe divulging information to another person "at the same covered entity or business associate."

to access protected health information and (ii) promptly deletes the e-mail upon realizing it was misdirected. The first exception applies to the recipient's impermissible access of protected health information (before deleting the e-mail) and the second exception applies to the inappropriate "disclosure" that occurred when the e-mail was accidently sent to the recipient.

3. **Recipient Does Not Retain Protected Health Information.** The Data Breach Rule also excludes from the definition of "breach" disclosures to an unauthorized person for which a covered entity or business associate has "a good faith belief that [the recipient] would not reasonably have been able to retain [the] information." HHS illustrates this exception by explaining that no breach occurs when EOBs inadvertently mailed to an incorrect address are returned, unopened, by the Post Office.

Notices Required

A covered entity that experiences a breach—that is, an impermissible use or disclosure of unsecured protected health information that meets the "harm threshold" and does not fit within an exception—must provide notice of the breach to each affected individual, to HHS, and, in some cases, the media. A business associate that experiences a breach must report the breach to the covered entity it serves. The Data Breach Rule dictates the manner in which the notices must be provided, the time frame for providing the notices, and the contents of the notices.

Notice to Individual. A covered entity that discovers a breach must provide notice to "each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of [the] breach." The notice must be provided "without unreasonable delay and in no case later than 60 calendar days after the discovery of [the] breach."

The notice must be in "plain language" and sent to the individual by first-class mail, unless the individual agrees to electronic notice. The notice must contain:

- A brief description of what happened;
- The types of information affected by the breach;
- Steps the individual may take to protect him/herself from potential harm resulting from the breach:
- A description of steps the covered entity is taking to investigate the breach, mitigate harm, and protect against future breaches; and

- Contact procedures for the individual to ask questions or obtain additional information, including a toll-free number, e-mail address, web site, or postal address.

When a covered entity has insufficient or out-of-date contact information for affected individuals, it must provide substitute notice "reasonably calculated to reach the individuals affected by the breach." If the covered entity has insufficient or out-of-date contact information for less than ten individuals, it may provide substitute notice by e-mail, telephone, or other means. If ten or more individuals are affected, the substitute notice must be provided using either (i) a conspicuous posting on the home page of the covered entity's website for 90 days or (ii) a conspicuous notice published in "major print or broadcast media" in areas where affected individuals likely reside. The substitute notice must include a toll-free number through which affected individuals may obtain information for at least 90 days.

Notice to Media. Covered entities must notify the media of breaches involving more than 500 residents of a State (or other jurisdiction, such as a county or city). The notice must go to "prominent media outlets serving the [applicable] State or jurisdiction" and contain the same information as the individual notice, described above. HHS explains that this notice is "intended to supplement, but not substitute for, individual notice" and anticipates "that most covered entities will provide notification to the media . . . in the form of a press release." The provision does not apply to all breaches affecting more than 500 individuals: for example, a breach involving 600 individuals, 400 of whom live in one State and 200 of whom live in another, does not require notice to the media, because the breach does not affect more than 500 residents of any one State.

Notice to HHS. A covered entity must provide notice of all security breaches to

When is Breach Discovered?

The Data Breach Rule's 60 calendar-day time limit for providing notice of a breach begins on the day a covered entity or business associate "discovers" the "breach." A "breach" is "discovered" when "any person, other than the person committing the breach, who is an employee, officer, or other agent of the covered entity [or business associate]" knows or reasonably should have known of the breach.

Investigation of Breach. HHS emphasizes that this means a "breach" is discovered "when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach."

Business Associates. HHS further explains that, with respect to a business associate acting as a covered entity's "agent," the covered entity "discovers" the breach on the day the business associate learns of the breach, no matter when the business associate informs the covered entity. With respect to a business associate acting as an independent contractor, however, the covered entity "discovers" the breach when the business associate reports the breach to the covered entity (or the covered entity otherwise learns of the breach).

HHS. The Data Breach Rule requires covered entities to maintain a log (or other documentation) of breaches involving less than 500 individuals and provide the log to HHS "not later than 60 calendar days after the end of each calendar year." HHS will publish instructions for the reports on its website. Breaches involving 500 or more individuals must be reported "contemporaneously with the [individual] notice" described above. Instructions for these large breach reports will also be published on HHS's website.

Notice by Business Associate. A business associate must provide notice of a breach to the covered entity it serves "without unreasonable delay and in no case later than 60 calendar days after discovery of [the] breach." The business associate must provide, "to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach." The business associate must also provide any other information about the breach that the covered entity needs to meet its own Data Breach Rule obligations with the original breach notice "or promptly thereafter as information becomes available."

The Data Breach Rule does not require a business associate to provide notice of a breach to affected individuals, the media, or HHS. Nevertheless, HHS stresses that the covered entity and the business associate should "consider which entity is in the best position to provide notice to the individual" and, if necessary, address respective responsibilities in the business associate agreement. Hence, for example, an insurer providing administrative services to a self-funded group health plan may be the appropriate entity to provide breach notice, even though it is the self-funded group health plan's obligation under the Data Breach Rule. (See the side bar on page 7 for explanation of when a covered entity "discovers" a business associate's breach for purposes of determining when notices are required.)

* * * * * * * * * *

For more information, please contact Tom Bixby at (608) 661-4310 or TBixby@tbixbylaw.com