Omnibus Rule Revises What Constitutes a “Breach” Under HIPAA/HITECH Breach Notification Requirements

May 2013

For additional information, please contact your Account Manager or Tony Sorrentino at 402.964.5470 or tsorrentino@ssgi.com

HIPAA’s “Omnibus Rule (the “Rule”), published on January 25, 2013, modified many parts of the HIPAA regulations, including those that require notification of breaches of unsecured protected health information (PHI) by covered entities and their business associates (the “Breach Regulations”). This Bulletin discusses the Breach Regulations, as modified by the Omnibus Rule, and will be referred to as “Final Breach Rules.” Compliance with the Final Breach Rules, as is the case with most other Omnibus Rule provisions, is required by September 23, 2013.

For more information about other aspects of the Omnibus Rule that apply to employer-sponsored group health plans, see our Bulletin dated March 2013, entitled “Strategic Direction for 2013 and Beyond: New HIPAA Omnibus Rule.”

GENERALLY

Breach Defined. The Final Breach Rules provide a specific definition of “breach,” and compliance with the breach notice obligations begins with understanding this definition and being able to identify “breaches.” A “breach” is defined as the (i) acquisition, access, use or disclosure (ii) of protected health information (iii) that is not permitted under the HIPAA Privacy Rule and (iv) compromises the security or privacy of the protected health information. Not every violation of the HIPAA Privacy Rule will constitute a breach for purposes of the Final Breach Rules.

“Unsecured” PHI. The notice obligations set forth in the Final Breach Rules arise only for breaches of “unsecured” PHI. PHI is “secured” for purposes of the Final Breach Rules only to the extent it is encrypted in accordance with the methodology specified by the Secretary of Health and Human Services (HHS). For PHI that is secured in that manner, the notice obligations set forth in the Final Breach Rules do not apply – even if there is an unauthorized use or disclosure (although other notice obligations may apply).

New Rule: Presumption of Breach. If PHI is acquired, accessed, used or disclosed in a manner that violates the HIPAA Privacy Rule, the Final Breach Rules require a rebuttable presumption of breach – that is, an entity must presume that such acquisition, access, use or disclosure has compromised the security or privacy of the PHI unless it can demonstrate that there is a low probability that the PHI has been compromised. This is in clear contrast to the old rule, which required no presumption and simply entailed an assessment of whether the use or disclosure poses a significant risk of financial, reputational...
or other harm to the individual. In assessing the probability that the PHI has been compromised, the Final Breach Rules list four factors that must be considered (see pages 3-4).

**Burden of Proof.** Covered entities have the burden of demonstrating that they satisfied the specific notice obligations following a “breach” as defined by the Final Breach Rules, or, if notice is not made following an unauthorized use or disclosure, that the unauthorized use or disclosure did not constitute a “breach.”

**PHI Only.** As a threshold matter, the Final Breach Rules are concerned only with breaches involving PHI. If the information is not PHI, there is no breach. Thus, de-identified information and employment records held by a covered entity in its role as employer are not PHI. Note that the Omnibus Rule removed the exception in the old rules (i.e., pre-Omnibus Rule) for certain limited data sets that exclude both birth dates and zip codes – under the Final Breach Rules, limited data sets are treated no differently than any other PHI.

**Acquisition, Access, Use or Disclosure.** To be a breach, there must be an “acquisition, access, use or disclosure” of unsecured PHI. These terms are broadly defined and encompass essentially any access, use or exchange of PHI (whether authorized or not). Although the regulations do not specifically define “acquisition and access,” HHS stated that they are to be interpreted by their plain meanings, and that each is encompassed within the current definitions of “use” and “disclosure.” “Use” is defined as the “sharing, employment, application, utilization, examination, or analysis of [PHI] within an entity that maintains such information.” “Disclosure” is defined as “the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.”

**Note:** A mere use or disclosure of PHI does not trigger a breach analysis if (i) the use or disclosure is permissible under HIPAA or (ii) the use or disclosure is subject to an exception.

**“Unsecured” PHI.** Only an acquisition, access, use or disclosure of “unsecured” PHI can trigger the notice obligations under the Final Breach Rules. “Unsecured” PHI is PHI that is not secured through the use of an approved encryption or destruction method that renders the PHI unusable, unreadable or indecipherable to unauthorized individuals. Conversely, only PHI secured in accordance with the Encryption Guidance is considered “unusable, unreadable, or indecipherable” for purposes of the Final Breach Rules. HHS has issued guidance on what types of encryption will fall within the safe harbor provision.

**The Encryption Guidance.** According to the Encryption Guidance, PHI is considered unusable, unreadable or indecipherable to unauthorized individuals if it has been encrypted by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key,” and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools must be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The Encryption Guidance identifies specific methods that HHS has determined, in accordance with statute, meet the standard.

**Note.** Access controls, by themselves, do not meet the standard set forth in the Encryption Guidance for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals. Thus, PHI is not necessarily “secure” even if it is accessible only to those who have an authorized password.

If a covered entity or business associate “secures” PHI in accordance with the rules, and an unauthorized use or disclosure is discovered, the specific notice obligations set forth in the Final Breach Rules do not apply because the PHI is considered “secure.” On the other hand, if some other method not specifically identified in the Encryption Guidance is used, then the PHI is not considered secure and
an unauthorized use or disclosure that constitutes a “breach” will give rise to the specific notice obligations set forth in the Final Breach Rules.

**Note.** HHS has emphasized that Encryption Guidance does nothing to modify a covered entity’s responsibilities with respect to HIPAA’s Security Rule, nor does it impose any new requirements upon covered entities to encrypt all PHI. A covered entity may be in compliance with HIPAA’s Security Rule even if it reasonably decides not to “secure” PHI in accordance with the Encryption Guidance and instead uses a comparable method to safeguard the information.

**Violation of HIPAA Privacy Rule.** An acquisition, access, use or disclosure of unsecured PHI will not give rise to a “breach” unless the acquisition, access, use or disclosure is a violation of HIPAA’s Privacy Rule (e.g., a violation of the minimum necessary rule). As was the case prior to the Omnibus Rule, a violation of HIPAA’s Security Rule does not itself constitute a potential breach under the Final Breach Rules, although such a violation may lead to a breach if it results in a use or disclosure of PHI that is not permitted under the Privacy Rule.

**Note.** A violation of HIPAA’s Privacy Rule will not rise to the level of a “breach” unless the rule violated relates to the use or disclosure of PHI. Thus, a violation of HIPAA’s administrative safeguards does not, in and of itself, give rise to a “breach,” but, much like a violation of the Security Rule, such a violation may lead to a breach.

**Compromise the Security or Privacy of PHI.** Even if it is established that a use or disclosure of unsecured PHI violates the Privacy Rule, a breach may not have occurred if the violation does not “compromise the security or privacy” of the PHI. However, as previously noted, an acquisition, access, use or disclosure of protected health information in a manner not permitted by HIPAA’s Privacy Rule is presumed, under the Final Breach Rules, to be a breach unless the entity demonstrates that there is a “low probability that the protected health information has been compromised.” The entity’s demonstration must be based on a risk assessment of all of the following factors:

i. **the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;** HHS has stated that this factor looks at the types of information involved, such as whether the disclosure involved information that is of a more sensitive nature. For example, with respect to financial information, this includes credit card numbers, social security numbers or other information that increases the risk of identity theft or financial fraud. With respect to clinical information, this may involve considering not only the nature of the services or other information, but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results). This assessment is intended to help entities determine the probability that PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient’s own interests. Additionally, HHS said that where there are few, if any, direct identifiers in the PHI involved, entities should determine the likelihood that the PHI could be re-identified based on the context and the ability to link the information with other available information (e.g., where diagnosis and discharge dates are involved, consider the likelihood of identification based on the specificity of the diagnosis, the size of the relevant community and the ability of the recipient of the PHI to use other available information to re-identify the individuals).

ii. **the unauthorized person who impermissibly used the protected health information or to whom the impermissible disclosure was made;** This factor considers whether the person who impermissibly (i.e., in violation of the Privacy Rule) uses or receives the PHI has obligations to protect the privacy or security of information. HHS stated that if, for example, PHI is impermissibly disclosed to another entity governed by the HIPAA Privacy and Security Rules there may be less risk of harm to the individual, because the recipient entity is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information. In contrast, if PHI is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the information, the risk of harm to the individual is much greater. HHS also stated that this assessment should also consider (as mentioned above for the first required
assessing) the risk of re-identification. For example, if information containing dates of healthcare
service and diagnoses of certain employees was impermissibly disclosed to their employer, the
employer may be able to determine that the information pertains to specific employees based on
other information available to the employer, such as dates of absence from work. In this case, there
may be more than a low probability that the protected health information has been compromised.
Other guidance recommended by HHS adds that the likelihood any unauthorized individual will
know the value of the information and either use the information or sell it to others may also
be a consideration.

iii. whether the protected health information was actually acquired or viewed; and
This factor considers whether the impermissibly used or disclosed PHI was actually acquired or
viewed or, alternatively, if only the opportunity existed for the PHI to be acquired or viewed. For
example, if a laptop computer was stolen and later recovered and a forensic analysis shows the PHI
on the computer was never accessed, viewed, acquired, transferred or otherwise compromised, the
entity could determine that the information was not actually acquired by an unauthorized individual,
even though the opportunity existed. In contrast, however, if a covered entity mailed information to the
wrong individual who opened the envelope and called the entity to say she received the information in
error, then, in this case, the unauthorized recipient viewed and acquired the information because she
opened and read the information to the extent that she recognized it was mailed to her in error.

iv. the extent to which the risk to the protected health information has been mitigated.
This factor considers the extent to which the risk to the PHI has been mitigated (such as by 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), and the extent and
efficacy of the mitigation. This assessment, when considered in combination with the assessment
regarding the unauthorized recipient of the information discussed above, may lead to different results
in terms of the risk to the PHI. For example, a covered entity may be able to obtain and rely on the
assurances of an employee, affiliated entity, business associate or another covered entity that the
entity or person destroyed information it received in error, while such assurances from certain third
parties may not be sufficient.

Other factors may also be considered where necessary in evaluating the overall probability that the PHI
has been compromised. Generally, these risk assessments must be thorough and completed in good
faith, and the conclusions reached must be reasonable. If an evaluation of the factors discussed above
fails to demonstrate there is a low probability that the PHI has been compromised, breach notification is
required. HHS notes, however, that a covered entity or business associate has the discretion to provide
the required notifications following an impermissible use or disclosure of PHI without evaluation of the
probability that the PHI has been compromised. HHS stated it will issue additional guidance to aid in
performing risk assessments with respect to frequently occurring scenarios.

Are There Any Exceptions to the Rule?
The Final Breach Rules provide three exceptions to the definition of “breach”:

i. any unintentional acquisition, access or use of protected PHI by a workforce member or person
acting under the authority of a covered entity or a business associate, if such acquisition, access or
use was made in good faith and within the scope of authority and does not result in further use or
disclosure in violation of the Privacy Rule;

The Final Breach Rules uses the term “workforce member” instead of “employees.” A “workforce
member” means “employees, volunteers, trainees, and other persons whose conduct, in the
performance of work for a covered entity, is under the direct control of such entity, whether or not they
are paid by the covered entity.” A person is acting under the “authority” of a covered entity or business
associate if he or she is acting on its behalf in accordance with common law agency principles.
This may include a workforce member of a covered entity, an employee of a business associate or a
business associate of a covered entity. Similarly, to determine whether the access, acquisition or use
was made “within the scope of authority,” the covered entity or business associate should consider whether the person was acting on its behalf at the time of the inadvertent acquisition, access or use.

In addition, while the statutory language provides that this exception applies where the recipient does not further use or disclose the information, HHS interprets this exception as encompassing circumstances where the recipient does not further use or disclose the information in a manner not permitted under the Privacy Rule. In circumstances where any further use or disclosure of the information is permissible under the Privacy Rule, there is no breach solely because of the further use or disclosure.

ii. any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized healthcare arrangement in which the covered entity participates, and the information is not further used or disclosed in violation of the Privacy Rule; and

As was the case before the Omnibus Rule, the Final Breach Rules modify the statutory language slightly to except from the definition of “breach” inadvertent disclosures of PHI from a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate or organized health care arrangement in which the covered entity participates.

HHS has clarified that “similarly situated individual” as used in the statute with regard to this second exception means an individual who is authorized to access PHI, even if that individual is not authorized to access the PHI at issue. For example, a physician who has authority to use or disclose PHI at a hospital by virtue of participating in an organized health care arrangement with the hospital is similarly situated to a nurse or billing employee at the hospital. In contrast, the physician is not similarly situated to an employee at the hospital who is not authorized to access PHI.

Additionally, HHS has clarified that “same facility” means the same covered entity, business associate or organized health care arrangement in which the covered entity participates, even if at a different location. Thus, if a covered entity has a single location, then the exception will apply to disclosures between a workforce member and, for example, a physician with staff privileges at that single location. However, if a covered entity has multiple locations across the country, the same exception will apply even if the workforce member makes the disclosure to a physician with staff privileges at a facility located in another state.

iii. a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

To illustrate this exception, HHS has used the following examples:

**Example 1:** A covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches.

**Example 2:** A nurse mistakenly hands a patient the discharge papers belonging to another patient, but she quickly realizes her mistake and recovers the PHI from the patient. If the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then this would not constitute a breach.
HHS has clarified that the applicability of any exception must be judged at the time a situation is judged and evaluated. Note that the Final Breach Rules removed the exception, available under the prior rule, for limited data sets not containing birth dates or zip codes.

**Are Any Changes to Our Privacy Policies and Procedures Required?**
Yes. Covered entities and business associates are required to comply with the administrative requirements of certain provisions of the Privacy Rule with respect to the breach notification provisions. These provisions, for example, require covered entities and business associates to develop and document policies and procedures, train workforce members on and have sanctions for failure to comply with these policies and procedures, permit individuals to file complaints regarding these policies and procedures or a failure to comply with them, and require covered entities to refrain from intimidating or retaliatory acts. Thus, a covered entity or business associate is required to consider and incorporate the requirements of the Breach Notification Rules with respect to its administrative compliance and other obligations.

**Who Has the Burden of Proof of Compliance?**
Covered entities and business associates have the burden of proof that they have satisfied their respective notice obligations under the Final Breach Rules. Thus, in the event of a “breach,” the covered entity must be able to prove that it notified affected individuals, the media and HHS, as required. Likewise, business associates must be able to prove that they notified covered entities of any breaches. If notice is not provided following an unauthorized use or disclosure, then the covered entity or business associate must be able to prove that the unauthorized use or disclosure was not a breach. Accordingly, when a covered entity or business associate knows of an impermissible use or disclosure of PHI, it should maintain documentation that all required notifications were made or, alternatively, of its risk assessment or the application of any exceptions to the definition of “breach,” to demonstrate that notification was not required.

**Note:** Covered entities are ultimately responsible for notifying affected individuals of a breach. This is true even if the breach occurs through or by a business associate that is also a covered entity. If an entity decides to delegate this responsibility to a business associate, the two entities should decide which is in the best position to do so.

**When Is a Breach “Discovered”?**
A breach is treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity or, by exercising reasonable diligence, would have been known to the covered entity. A covered entity is deemed to have knowledge of a breach if the breach is known (or by exercising reasonable diligence would have been known) to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity. Thus, a breach is deemed to be discovered at any point any workforce member or agent of the covered entity knows, or should have known, of its existence.

**Note:** This provision has a very broad concept of “discovery.” Make sure to have proper training and channels of communication (both within the entity and between business associates and covered entities), so that the correct officials are quickly alerted when a breach has been “discovered” for purposes of this rule.
ACTION PLAN

Establish or Update Breach Identification Procedures. Covered entities and business associates should already have breach identification procedures, but it is important to make sure that they are compliant with the Final Breach Rules.
- Determine whether there has been an impermissible use or disclosure of PHI under the Privacy Rule.
- Undertake a risk assessment and document the results.
- Determine whether the incident falls under one of the three exceptions to the breach definition.

Establish or Update Breach Notification Procedures. Covered entities and business associates should determine which breach notification must be sent (i.e., individual notices, substitute notices, immediate notices to HHS, media notices, notices from business associates to covered entities) and who will be responsible for gathering the necessary information for such notification, preparing the notices and sending the notices.

Document Breaches for HHS Reporting. For breaches of unsecured PHI involving 500 or more individuals, entities must notify the Secretary contemporaneously with the individuals. For breaches of unsecured PHI involving fewer than 500 individuals, a covered entity must maintain a log or other documentation of such breaches and notify HHS not later than 60 days after the end of each calendar year about breaches discovered during the previous calendar year.

Amend Business Associate Agreements. Covered entities and business associates should coordinate their breach notification efforts in order to avoid duplicate notices and to ensure efficiency with regard to information gathering and time frames. Covered entities whose business associates act as agents of the covered entity should consider requiring business associates to notify the covered entity of a breach discovery well in advance of the 60-day deadline provided in the Final Breach Rules, as the breach discovery date of an agent is treated as the breach discovery date of the covered entity for purposes of providing timely notices to individuals and, if required, HHS and the media.

Workforce Training. The clock for sending breach notifications begins to tick as soon as a breach is known (or, by exercising reasonable diligence, would have been known) to any workforce member or agent (other than the person committing the breach) of the covered entity. Covered entities and business associates will want to enhance training so that their employees are aware of the importance of timely reporting of privacy and security incidents, and of the consequences of failing to do so.

Administrative Requirements — Revise Policies and Procedures, Training, Sanctions, Complaint Process. Covered entities must incorporate the requirements of the Final Breach Rules into their policies and procedures, and workforce training sanctions must be developed for failure to comply, as well as a complaint process for failures to comply with these new policies and procedures.

Covered entities and business associates should consult legal counsel to work through these steps to ensure that breach notification is provided when required.