wiley

ARTICLE

Summary of the New HIPAA/HITECH Omnibus Regulation

January 28, 2013

After almost four years, the Department of Health and Human Services (HHS) finally has released its "omnibus" Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act regulation, implementing changes to the HIPAA Privacy, Security and Enforcement Rules, as well as the interim final regulation on breach notification and certain changes to the Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA). The regulation was published in the Federal Register on January 25, 2013. See 78 Fed. Reg. 5566 (Jan. 25, 2013), available here.

This article describes the highlights of these new provisions. Most of these provisions are not "new," as they implement specific HITECH provisions and adopt the elements of the earlier proposed rule from July 2010.

Nonetheless, these provisions are quite important for the entire health care industry, including HIPAA covered entities, business associates of these covered entities, downstream contractors of these business associates and a wide variety of entities who otherwise use and disclose health-related information. There are a number of important new compliance obligations and challenges, for both covered entities and business associates, as well as several new issues to evaluate.

The final rule is "effective" on March 26, 2013. Covered entities and business associates must comply with the new provisions by September 23, 2013 (180 days after the effective date).

Practice Areas

Health Care

Privacy, Cyber & Data Governance

The Breach Notification Standard

The provision of the omnibus regulation that has generated the most discussion so far—and that will have the most substantial impact on the overall health care community—is the elimination of the "risk of harm" standard for breach notification. While most of the provisions of the "interim final" breach notification regulation have not changed—and HIPAA covered entities and business associates have been following these provisions for more than two years— the omnibus regulation changes the "trigger" for when notification is required.

Specifically, HHS has eliminated the "risk of harm" standard that was implemented in the interim final rule. Under this provision, notification was required for individuals when the breach involved a "significant risk of financial, reputational or other harm" for the individual.

However, while this "risk of harm" standard has been eliminated, it is critical for covered entities and business associates to understand that, while this requirement has been eliminated, an alternative approach has been implemented that will result—in most but clearly not all situations—in the same conclusions about notification.

There are two key steps in the changes implemented by HHS. First, HHS has clarified that the "presumption" is that a breach requires notification to the affected individuals unless the covered entity "demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment." This change was designed to ensure that companies did not use the absence of clear information about a breach as a basis for a "no notice" decision. It is now explicit that notice is required unless a covered entity can conclude there is a "low probability" of "compromise" of the data.

Second, HHS has replaced the "risk of harm" threshold with a more precise "risk assessment" designed to determine whether there is a "low probability" of "compromise" of the data. While there is no longer a specific definition of this idea of "compromise," the set of factors for the risk assessment indicates that the analysis made by a covered entity will be very similar to what is being done today. Specifically, a covered entity, as part of its risk assessment, must review the following factors (along with any others that are appropriate):

(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 the protected health information has been mitigated.

Obviously, there are differences in the approach, because HHS has stated that there are differences. However, because companies are required to conduct this risk assessment (unless a company wants to provide notice without any risk assessment), the final standard primarily implements a variation on the risk investigation that has been conducted over the past two years.

Key Breach Notification Points to Consider

- No "Bright Line" on Breaches
  HHS is not requiring notification every time there is a "breach." It rejected the call to require a "bright line" standard that would trigger notification every time. HHS continues to believe that "a risk assessment is necessary," and that there are situations where a specific breach incident "is so inconsequential that it does not warrant notification." HHS also "agree[s] with commenters that providing notification in such cases may cause the individual unnecessary anxiety or even eventual apathy if notifications of these types of incidents are sent routinely."
- The Standard Is Different But . . .
  There are differences in the final standard. However, because the final regulation replaces a "risk of harm" definition with a "risk assessment" that factors in many of the same elements, there are strong reasons to believe that the new standard will not result in material differences in the notification of breaches in many situations.
- Use the Compliance Period Wisely to Learn the New Standard
  Companies should use the compliance period over the next several months to evaluate potential breaches using both standards, to identify and resolve situations where the company believes that different results will be required under the different standards. *Be very careful before concluding that no notice will be provided in a situation where the covered entity concludes that notice is not required under the "risk of harm" standard but will be required after the compliance date under the new standard.* It also will be important—once the compliance period has ended—to pay close attention to any additional guidance on this issue from HHS and any early enforcement efforts related to this standard.

Impact on Business Associates

While the substantive impact of the new breach notification regulation will create enormous effects because of the continuing prevalence of security breaches in the health care industry, *the most substantial compliance impact from the regulation will be on the business associate community.* While these changes are substantial, they are essentially the same "new" obligations that business associates should have been aware of since the passage of the HITECH law in 2009. Now, business associates have a specific timetable to get into compliance with these provisions.

- Business Associate Privacy Rule Obligations
  The omnibus regulation addresses a variety of issues dealing with business associates. First, the regulation implements the HITECH provision that business associates now will have a legal obligation to comply with the required provisions of a business associate contract under the Privacy Rule. For business associates, this change should not affect behavior (since business associates already should have been following their contractual obligations under the business associate contracts), but now creates legal exposure for violations. The regulation makes clear that business associates do not need to comply with all provisions of the Privacy Rule (such as providing a privacy notice), but only those

provisions that are incorporated into a standard business associate agreement.

- Business Associate Security Rule Obligations
  The regulation also now requires business associates to comply in full with the HIPAA Security Rule. This is an enormous new obligation. Today, under business associate contracts, business associates have an obligation to implement reasonable administrative, technical and physical safeguards to protect electronic protected health information. Under the new provisions, business associates will need to comply with the full HIPAA Security Rule. This is a significant additional step in security compliance that will affect an enormous number of business associates. Moreover, this is one of the HIPAA requirements that takes both time and resources—to evaluate security programs, conduct an appropriate risk assessment, implement risk management strategies and prepare appropriate written policies and procedures encompassing a full information security program.
- A Business Associate Has Obligations Even Without a Contract
  HHS also has made clear that the question of whether an entity is a business associate or not is a legal question, not simply a matter of contract. This means that the obligations of a business associate are imposed by law, whether or not an appropriate business associate contract is in place.
- Conduits
  The new definitions of "business associate" (which adds in certain entities like health information organizations) incorporates the idea of a "conduit," although it still leaves some open questions about certain entities that solely transmit data for a short, finite period of time (following the prototype "conduit" example of the US post office). However, to clarify a misunderstanding from the proposed rule, HHS states that entities that "maintain" data, even if they do not routinely access it, are considered to be business associates. The rule makes clear that the "conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services." An entity that "maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information." This means that entities such as document storage companies—who "maintain" data even if they never access it—are business associates.
- Subcontractors
  The regulation also makes clear that downstream subcontractors of business associates are covered as business associates. This is a significant issue, as it broadens substantially the range of entities affected by these regulations as business associates. The idea is that any entity that receives or has access to PHI in the course of the downstream relationship will be considered a business associate.
- Transition Periods
  HHS has developed a specific transition period for revised business associate agreements that incorporate these new standards. Essentially, if an appropriate business associate agreement is in place as of the publication date of the omnibus rule (January 25, 2013), then there is an additional period of one year beyond the compliance date of September 23, 2013 to revise business associate agreements to remain in compliance. This transition applies only to the revised agreements themselves —business associates still must comply with the applicable HIPAA provisions as of the compliance date

for the regulation.

Key Business Associate Points to Consider

- For business associates, develop a plan to implement the HIPAA Security Rule. This takes time and resources.
- Review your privacy rule compliance actions. Your obligations do not substantively change, but some business associates have not always paid close attention to these contractual obligations.
- Develop a contracting process and approach for now and over the next two years.
- Both business associates and covered entities should evaluate how they wish to implement these provisions in business associate contracts. While there is no formal requirement to redo a business associate agreement, it is very unlikely that existing agreements will incorporate all required elements of this new omnibus regulation.
- Evaluate the "agent" idea, which affects both the covered entity's potential responsibility for the actions of the business associate as well as various other elements. This analysis is very "fact specific," and may be hard to generalize in any meaningful way (and may even change for a particular business associate depending on the projects assigned to a business associate over time). Therefore, both covered entities and business associates should evaluate how it wishes to addresses this "agent" idea.

The HIPAA Enforcement Rule

The omnibus regulation contains many changes to the HIPAA enforcement rule. Most of these changes are spelled out in the statute and are not changed in material ways from the proposed rule. For the most part, the final provisions spell out a very complicated set of procedures for a formal enforcement process that are almost never used (or have not been to date). In addition, while HHS goes out of its way to define details in the process, it also is clear that HHS has enormous flexibility in its investigations, both as to whether and how to conduct an investigation and in how an investigation will be resolved. For example, there are particular limits on the penalties that can be applied and several "tiers" of penalties defined by the statute, but HHS has defined these limits in a way that allows it (in an appropriate situation) to implement fines at virtually any level for virtually any category of violation, depending on how a violation is categorized in the course of the investigation. Accordingly, *when companies are faced with an investigation, they will want to review these procedures in detail, but there are few direct compliance issues created by these changes to the enforcement rules.*

Marketing Provisions

The final rule implements two important changes to the marketing rules under HIPAA.

First, HHS implements the requirement that is designed to restrict marketing that is permitted without authorization where the covered entity receives "remuneration" for the marketing. Based on the final rule, if a marketing communication had been permitted in the past without an authorization (obviously, marketing was very restricted already under the original HIPAA rules), but the covered entity (or business associate) received

remuneration for making the communication, the communication could no longer be made without an authorization. This applies to both "direct" and "indirect" remuneration, but does not apply to "non-financial benefits, such as in-kind benefits, provided to a covered entity in exchange for making a communication about a product or service."

On a related note, HHS also discussed certain payments that are still permitted for certain "refill" communications, but these payments are limited to "reasonable costs" and do not permit a covered entity to make a profit for sending the communication.

Second, unlike in the proposed rule, HHS decided to limit the exceptions to this rule, so that authorization is required for all treatment and health care operations communications where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being marketed. The proposed rule had proposed an "opt-out" for certain treatment communications, but ultimately decided that too much confusion was created by this exception. Therefore, it concludes in the final regulation that "requiring authorizations for all subsidized communications that market a health related product or service is the best policy."

- Key Point - Identify any situation where these marketing provisions may be implicated, particularly where a covered entity is marketing some product or service offered by another entity. If you receive any kind of payment in connection with a marketing communication, you should analyze these activities under this new standard.

Sale of PHI

Similarly, HHS implemented the HITECH requirement that prohibits the sale of protected health information without individual authorization. For many companies, this provision may be of little relevance, as many companies do not sell PHI. For those companies for whom this issue is relevant, this new provision substantially restricts the ability to sell PHI—to the extent that the sale has been permitted in the past under the existing rules. Absent a relevant exception, there can be no sale of PHI without an individual authorization. This prohibition applies to both financial and nonfinancial benefits, and therefore may require companies to evaluate a variety of situations where there is some category of "in kind" benefit from data disclosures.

The exceptions cover a variety of different areas, including (a) public health activities; (b) research purposes, but only where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information; (c) treatment and payment purposes; and various other exceptions. In these situations, covered entities can continue to receive remuneration for disclosures for these purposes. To the extent companies receive remuneration in connection with providing PHI to another entity, this new provision should encourage an evaluation of whether the disclosure is permitted without the need for patient authorization.

- Key Point - Analyze any situation in which you receive any kind of benefit for making a use or disclosure of PHI. Some of these may be easy to identify (e.g., a company doing research pays for data in connection with otherwise compliant research). Others may be more complicated (data is shared in

exchange for some kind of other resource, including reports based on the data). All of these exchanges will need to be evaluated under this new standard.

Privacy Notices

The new regulations require various changes to privacy notices. Every covered entity will want to review its existing notice, and make changes both as required by the regulation and in general, to reflect any changes in business operations since the notices were last prepared.

The rule requires additions of materials about situations where an authorization is required (such as marketing), disclosure about fundraising communications (if made) and the right to request the restriction on disclosures for self-pay items or services, as well as the right of individuals to be notified in the event of certain security breaches (as defined by the breach notification regulation).

Aside from the substance of the notice changes, the other primary issue with new notices involves the distribution of these notices. HHS has determined that these new requirements are "material" and that new distribution of notices will be required. Health plans generally will be permitted to post their new notices on their web sites as of the compliance date, and will be able to provide "a revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan" (meaning that a separate distribution of the notice is not required). Health care providers must post the notice in a "clear and prominent" location, must continue to provide the notice to new patients and must provide it to other patients on request.

Authorizations – Research

HHS has proposed certain changes to the authorization requirements to make certain kinds of research-related authorizations more feasible.

The final regulation allows a covered entity to combine "conditioned" (typically where treatment is conditioned on participating in a research project) and unconditioned research projects into a single authorization form, "provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities." Covered entities, research entities and the related privacy or institutional review boards examining research proposals are given "flexibility" to design the best way of informing individuals about these options.

The final regulation also modifies a prior interpretation of the research authorization, so that "future" research projects can be part of an authorization as well. As part of an ongoing effort to improve research opportunities through the HIPAA rules, future research projects now can be included in an authorization as long as the authorization "adequately describe[s] such purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research."

GINA Issues

The GINA law required a change to the Privacy Rule to prohibit "a covered entity that is a group health plan, health insurance issuer that issues health insurance coverage, or issuer of a medicare [sic] supplemental policy" from using or disclosing genetic information for underwriting purposes. The final regulation does that. It applies this concept more broadly to all HIPAA "health plans," with the exception of long term care policies. The provision also ensures that "genetic information" is included in the definition of protected health information.

Miscellaneous

The omnibus regulation contains a number of other provisions, many of them simply taken almost verbatim from the HITECH statute. Some of the more important of these "miscellaneous" provisions include:

- Expanding the Individual Access Right
  One of the few provisions where HITECH focuses on the idea of "electronic health records" is in connection with the changes to the HIPAA access right. While the HITECH statute discussed providing electronic access to electronic health records, the final regulation requires provision of access to an electronic copy of all electronic information in a designated record set, where feasible. Covered entities have reasonable flexibility to identify an appropriate electronic format for access, and are not required to convert non-electronic materials into electronic documents. HHS has modified the timeframe for producing electronic records somewhat (by emphasizing the need for a thirty day production), but rejected efforts to reduce this time for production more substantially.
- New Obligations to Restrict Disclosure When the Individual Has Paid Out of Pocket.
  One of the more confusing HITECH provisions involves the right of individuals to request that health care providers restrict disclosure of information to health plans in situations where the patient has paid for an item or service in full. Under the HITECH law and the new regulations, providers are forced to agree to this request in this situation. This has created concern about how this provision is to be implemented, particularly where a particular item is connected to an ongoing course of treatment. There also is considerable concern among some fraud investigators that this provision is an invitation for patients to commit fraud by hiding certain information from the health plans.

  The final regulation implements these requirements. HHS has tried to clarify the obligations of providers (for example, there is no obligation to create separate medical records but there is a need to flag these items or services in the existing record). This is an area that healthcare providers will need to pay some particular attention to, in terms of developing appropriate procedures (although the volume of this issue arising is very unclear).

  In general, this provision may turn out to have little application, as there are many ways today to hide specific treatment from health insurers. Moreover, because the threshold requirement is that treatment be paid for in full, there are limited circumstances where an individual would choose to avoid having

an insurer make payments where insurance is in place. Nonetheless, for health care providers, it will be important to develop a process to accept these requests and to develop an ongoing means of protecting this information on a going forward basis. This provision does not impose any compliance obligations on health plans, but health plans should evaluate whether there are situations where this lack of information could create concerns.

- Fundraising
  The final regulation makes modest changes to the fundraising provisions, as required by the HITECH statute. Essentially, the regulation (1) clarifies that a clear and explicit opt-out must be included with all fundraising communication (to allow individuals to opt-out of future fundraising), and (2) expands somewhat the information that can be used in connection with fundraising activities (to permit reasonable targeting of fundraising communications).