Bloomberg BNA

Health Insurance Report™

VOL. 19, NO. 14 APRIL 3, 2013

Four Key Areas of the New HIPAA Privacy Regulations




BY ROSS FRIEDBERG, ROBERT HUDOCK, ADAM SOLANDER, AND PATRICIA WAGNER

On January 25, 2013, the Health Insurance Portability and Accountability Act ("HIPAA") regulations (the "Omnibus Rule") implementing the statutory amendments under the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") were published in the *Federal Register*.[1] The Omnibus Rule is effective March 26, 2013, but covered entities and business associates have until September 23, 2013, to comply with most of the new requirements. In addition to a number of administrative requirements (such as the requirement that a Covered Entity[2] modify its Notice of Privacy Practices), the Omnibus Rule likely is to have its greatest impact in the four areas discussed below.

Friedberg is an associate in Epstein Becker & Green PC's Health Care and Life Sciences practice in the firm's Washington office. He can be reached at RFriedberg@ebglaw.com. Hudock is a member in the Health Care and Life Sciences practice in the firm's Washington office and practices in the firm's E-Health Group. He can be reached at rhudock@ebglaw.com. Solander is an associate in the Health Care and Life Sciences practice in the firm's Washington office. He can be reached at ASolander@ebglaw.com. Wagner is a member in the Health Care and Life Sciences and Litigation practices in the firm's Washington office. She can be reached at pwagner@ebglaw.com.

Compliance with all aspects of the Omnibus Rule is critical; however, the four areas discussed below may have the greatest impact (in terms of privacy compliance) in the health care industry. Specifically:

1. The new breach reporting standards will need to be incorporated into policies and procedures. It is ex-

[1] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Department of Health and Human Services, Office of the Secretary (45 C.F.R. Parts 160 and 164). 78 Fed. Reg. 5566 (Jan. 25, 2013).

[2] 45 C.F.R. 160.103.

 ISSN 2154-8986

pected that the new standard will result in additional reporting. As a result, organizations will need to anticipate additional costs associated with reporting.

2. Changes to the marketing rules will require not only a change to policies and procedures but a thoughtful analysis of current business relationships.

3. There is a potential that business associates will be ''deemed'' an agent of the covered entity, thus exposing the covered entity to additional liability. In determining the impact of increased potential exposure for acts of business associates, covered entities and business associates will need to evaluate their business associate arrangements, assess risks and exposure, and take steps to mitigate those risks as much as possible.

4. Business associates will need to undertake the time-consuming process of ensuring that all subcontractors have entered into, and understand the implications of, business associate relationships.

1. Revised Breach Reporting Standard

The Omnibus Rule[3] replaces the current ''significant risk of harm'' standard with a ''low probability of compromise'' standard for determining whether a security incident is reportable. Similar to the Interim Final Rule,[4] security breaches involving 500 or more individuals must be reported to the Secretary of the Department of Health and Human Services (''HHS'') immediately (concurrently with notification of the individuals). A security breach involving less than 500 individuals must be reported to the Secretary of HHS within 60 days following the end of the year in which the breach occurred.

Business associates will need to undertake the time-consuming process of ensuring that all subcontractors have entered into, and understand the implications of, business associate relationships.

Until September 23, 2013, covered entities must continue to comply with the interim final rule for breach notification. The Preamble to the Omnibus Rule (the ''Preamble'') states: ''Thus, during the 180 day period before compliance with this final rule is required, covered entities and business associates are still required to comply with the breach notification requirements under the HITECH Act and must continue to comply with the requirements of the interim final rule.''[5]

However, after September 23, 2013, covered entities and business associates must utilize the new standard of the Omnibus Rule. Under this new standard, there is presumption that any unauthorized use, disclosure, or access to protected health information (''PHI'') is a reportable breach. Thus, the covered entity and/or business associate must provide notice of an unauthorized use, disclosure, and/or acquisition of PHI absent a finding that there is a ''low probability that the [PHI] has been compromised.''

For example, as described in the Preamble, the inappropriate mailing of Explanation of Benefits (''EOB'') data consisting of names, dates of service, and amounts paid would be a reportable breach, absent other mitigating factors. The Preamble notes that this new standard is intended to address the Secretary of the HHS's concern that ''some may have interpreted the risk of harm standard in the interim final rule as setting a much higher threshold for breach notification than [HHS] intended to set.''[6]

In describing the ''new'' analysis, the Preamble emphasizes that this analysis is different than the risk-of-harm analysis used under the Interim Final Rule. Under the Interim Final Rule, to determine whether a breach was reportable, covered entities and business associates asked the following question: ''Is there significant risk of harm?'' Under the Omnibus Rule, this question will be replaced with, ''Is there a low probability of compromise?''

The Omnibus Rule identifies four factors that must be addressed during the covered entity/business associate's risk analysis. However, a covered entity/business associate may elect to notify without conducting a risk analysis.

The First Factor: Nature and Extent of PHI Involved

The first factor requires a consideration of the ''nature and extent of the PHI involved, including the types of identifiers'' as well as the likelihood of re-identification. This is necessary because breaches involving limited data sets that do not contain birth dates and/or zip codes, which previously were not reportable, are now reportable under the Omnibus Rule. The Omnibus Rule requires the use of a new ''low probability of compromise'' risk analysis approach to determine whether a breach involving a limited data set must be reported (absent another explicit exception). Under this approach, determining that the risk of harm is low does not remove an incident from the reportable to the not-reportable category unless the probability of compromise also is low.

The Second Factor: Capabilities of Unauthorized Recipient

The second factor under the new standard requires that the covered entity and/or business associate develop a profile and assess the capabilities of the unauthorized recipient of the PHI (e.g., professional, legal, technical skill, etc.). This analysis presumably would entail considering specific facts about the person or persons that either restrict or enhance the ability of the unauthorized person to exploit (compromise) the PHI.

The Preamble provides an example of information maintained in a data base containing only the dates of health care service and diagnoses being impermissibly disclosed to an employer. Even without the presence of employee names, the Preamble opines that the disclosure presents more than a low probability of compromise. The Preamble explains that because the employer

[3] *Id*.
[4] 74 Fed. Reg. 42740 (Aug. 24, 2009).
[5] 78 Fed. Reg. 5566, 5570.
[6] 78 Fed. Reg. 5566, 5641.

  HIR ISSN 2154-8986

might be able to determine which employees were affected based on other information available to the employer (such as absences from work).[7]

The Third Factor: Evidence the PHI Was Never Compromised

The third factor allows for the possibility of establishing that PHI, once re-secured, was never actually copied, used, viewed, or otherwise compromised. The classic scenario, cited by HHS on numerous occasions, involves the loss of a laptop that is subsequently reacquired. In this instance, the covered entity and/or the business associate may rely on a forensic analysis to establish that PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised. Based on such an analysis, the covered entity and/or business associate may reasonably determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed.

The Fourth Factor: Mitigation of Risk

The fourth factor considers the extent to which the risk to PHI has been mitigated. For example, a covered entity and/or business associate may 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. However, the Preamble cautions that ''assurances from certain third parties may not be sufficient.''

Exception to the Breach Standard

As in the Interim Final Rule, the Omnibus Rule maintains the following exceptions whereby a covered entity or business associate may conclude that no breach has occurred without having to conduct a risk analysis:

- The PHI was secured (e.g. through encryption or some similar device). By definition, PHI encrypted using an approved methodology cannot be accessed, used, or disclosed (assuming the encryption key has not been otherwise compromised). While the method prescribed for securing information remains the same, the software and hardware that meets this standard periodically changes. New software and hardware becomes certified and other software and hardware loses certification because of security vulnerabilities (refer to http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm for more information). Similarly, PHI located on a device destroyed using an approved methodology is also not reportable.

- The unintentional access, use, or disclosure of PHI by a person acting under the authority of the covered entity and/or business associate (where the access, use, or disclosure) was done in good faith and within the course and scope of relationship;

- The inadvertent disclosure from one person authorized to access, use, or disclose PHI occurs within the same facility, operated by covered entity or business associate, and the person to whom the information was disclosed is similarly situated; and

- The unauthorized disclosure of PHI where the person cannot reasonably retain the information.[8]

Given the changes, the Omnibus Rule's replacement of the ''significant risk of harm'' standard with a ''low probability of compromise'' standard will require covered entities and business associates to put in place new policies and procedures to guide their organizations in analyzing potential breaches. As noted above, it is anticipated that the new analysis will increase the number of events that are reportable as breaches.

2. Imposition of New Restrictions on Using PHI for Marketing Purposes

Among the many privacy law changes brought by the Omnibus Rule are changes to the Privacy Rule relating to the use of PHI in marketing communications. The Privacy Rule has always required covered entities to obtain written authorization from individuals before disclosing PHI in a marketing communication, subject to certain exceptions relating to treatment, health care operations, and certain other activities.

The Omnibus Rule, by expanding the definition of ''marketing'' to include some communications that previously were excluded from the definition, significantly expands the range of marketing activities that require a prior written authorization.

Because ''marketing'' encompasses such a broad range of activities, these changes should be considered among the most significant of the recent changes to the Privacy Rule and will have widespread impact on the business practices of health plans, health care providers, and their business associates.

Modification of General Exclusion for Communications Relating to Treatment and Health Care Operations

The Privacy Rule defined ''marketing'' broadly to include any communication about a product or service that encourages recipients of the communication to purchase or use the product or service. However, excluded from the broad definition were certain communications relating to treatment, health care operations, as well as certain other activities, such as care coordination.

The Omnibus Rule significantly modifies the marketing definition by limiting these exceptions to only those communications that were NOT made in exchange for remuneration from a third party (referred herein as ''subsidized communications''). Among the types of subsidized communications that will now require individual authorization are those communications directly (or indirectly) paid for by third parties (e.g., being paid by a drug manufacturer to communicate information about a new drug).

Consistent with other provisions in the Omnibus Rule that impose heightened responsibilities on business associates, the marketing restriction on subsidized communications clearly applies to both business associates and covered entities. As explained in the Preamble:

> Even where a business associate of a covered entity, such as a mailing house, rather than the covered entity itself, receives the financial remuneration from the entity whose product or service is being promoted to health plan members, the communication is a market-

[7] 78 Fed. Reg. 5643.

[8] 78 Fed. Reg. 5639.

> ing communication for which prior authorization is required.[9]

However, the restriction for subsidized communications does not apply in all cases. There are two types of circumstances where subsidized communications will not fall under the marketing definition.

The first type involves circumstances where the ''remuneration'' provided in exchange for the communication is an in-kind benefit (e.g., distributing marketing materials to patients that were provided, at no cost, from a third party); and the second type involves circumstances where payments are made for a non-marketing purpose, such as to implement a treatment or care coordination program, and the communication is about the program itself. Regarding the latter, the Preamble emphasizes the importance of the distinction between subsidized communications made for marketing and non-marketing purposes:

> We continue to emphasize that the financial remuneration a covered entity receives from a third party must be for the purpose of making a communication and such communication must encourage individuals to purchase or use the third party's product or service. If the financial remuneration received by the covered entity is for any purpose other than for making the communication, then this marketing provision does not apply.[10]

Additionally, it's important to note that the Privacy Rule's marketing requirements apply only to communications that involve the use or disclosure of PHI, such as communications directed at specific individuals or groups based on their health or health plan membership status. If the communication does not involve the use or disclosure of PHI, then the marketing restriction in the Privacy Rule will not apply.

Other Exceptions to Marketing

The Omnibus Rule also creates a separate exclusion from the definition of ''marketing'' for prescription drug refill reminders. But unlike the general exclusion for marketing communications that relate to treatment, this exclusion covers subsidized communications relating to refills so long as the payment received by the covered entity is ''reasonably related to the covered entity's cost of making the communication.'' Refill reminders are broadly interpreted as including communications about generic equivalents, communications encouraging individuals to take their prescribed medications, and communications relating to all aspects of a self-administered drug delivery system, such as insulin pumps.

Content of the Authorization for Subsidized Communications

When a subsidized communication requires an individual's written authorization, covered entities (or their business associates) will need to include certain information on the authorization form relating to the remuneration that will be received. Specifically, the authorization must:

- disclose the fact that the communication is subsidized by a third party;
- describe the intended purpose of the authorization (i.e., why it is being sought); and
- meet all other requirements generally applicable to authorizations required under the Privacy Rule.

However, the authorization required for subsidized communications does not need to disclose the specific products or services being marketed. As explained in the Preamble, an authorization that describes unspecified subsidized communications will be sufficient to meet the authorization requirements as long as all other authorization requirements are met.[11]

3. Potential Increase in Liability to Covered Entities for Acts of Business Associates

Another significant change from the Omnibus Rule is the increased potential for covered entities to be liable for acts of business associates. While the enforcement provisions of the Privacy Rule previously provided that a covered entity would be liable (in accordance with the federal common law of agency) for the acts or omissions of an agent (provided the agent was acting within the scope of its agency), an exception was made for business associates. Under this exception, a covered entity was not liable for the acts or omissions of business associates if the covered entity had: (1) complied with administrative safeguards as well as use and disclosure requirements with respect to the business associate, and (2) did not know of the pattern or practice of the business associate at issue and failed to act as required by the Privacy Rule.[12]

The Omnibus Rule removes this exception, making covered entities liable for the acts of business associates, even where the covered entity has complied with its contractual obligations and had no knowledge of the wrongdoing.

Thus, under the Omnibus Rule, the threshold question will be whether the business associate is an ''agent'' as determined under the federal common law of agency. The Preamble makes clear that mere labels will not suffice for the analysis:

> The terms, statements, or labels given to parties (e.g., independent contractor) do not control whether an agency relationship exists. Rather, the manner and method in which a covered entity actually controls the service provided decides the analysis.[13]

The Preamble further provides that the analysis of whether a business associate is an agent will be fact specific depending on factors such as:

(1) the time, place, and purpose of a business associate's conduct;

(2) whether a business associate engaged in a course of conduct subject to a covered entity's control;

(3) whether a business associate's conduct is commonly done by a business associate to accomplish the service performed on behalf of a covered entity; and

[9] 78 Fed. Reg. 5597.
[10] *Id.* at 5596.
[11] *Id.*
[12] 45 C.F.R. § 160.402(c).
[13] 78 Fed. Reg. 5581.

  HIR ISSN 2154-8986

(4) whether or not the covered entity reasonably expected that a business associate would engage in the conduct in question.[14]

The Preamble also notes that the authority of a covered entity to ''give interim instructions or direction'' is the type of control that will be a distinguishing factor in the analysis. For example, if the covered entity retains the authority to dictate how a business associate must make information available to the covered entity in order to fulfill an individual's request for access, an agency relationship may exist. Although the Preamble also notes that there are some business associate relationships that are unlikely to create an agency relationship (e.g., accreditation services), other business associate relationships (and subcontractor relationships of for business associates) will have to be evaluated on a case-by-case basis.

The agency relationship also permeates the requirements of breach reporting, as the Preamble states that timing for breach notification when the breach involves a business associate is dependent on whether the business associate is an agent of the covered entity. Specifically, the Preamble provides:

> With respect to timing [for breach notification], if a business associate is acting as an agent of a covered entity, then, . . . the business associate's discovery of the breach will be imputed to the covered entity. In such circumstances, the covered entity must provide notifications . . . based on the time the business associate discovers the breach, not from the time the business associate notifies the covered entity. In contrast, if the business associate is not an agent of the covered entity, then the covered entity is required to provide notification based on the time the business associate notifies the covered entity of the breach.[15]

This Omnibus Rule change could have a significant impact on business associate and covered entity relationships, as covered entities evaluate the potential for liability. Business associates likely will be conducting the same evaluation of any vendors that the business associate utilizes.

4. Direct Liability to Business Associates

Finally, as was anticipated, the Omnibus Rule makes clear the direct liability that flows to business associates as a result of the modifications to the HITECH Act. In addition, the Omnibus Rule explicitly includes e-prescribing gateways and other electronic health record vendors as business associates.

The Preamble states that a business associate is directly liable for:

- uses and disclosures of PHI that violate its business associate agreement or the Privacy Rule;
- failing to disclose PHI when the Secretary of the HHS requires it to do so, or when an individual requests an electronic copy of PHI;
- failing to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request; and
- failing to enter into business associate agreements with subcontractors that create or receive PHI on their behalf.[16]

Notable among the above list is the requirement that business associates enter into business associate agreements with subcontractors.

The Omnibus Rule extends the business associate designation to subcontractors of business associates by explicitly expanding the definition of ''business associates'' to include ''a subcontractor that creates, receives, maintains, or transmits [PHI] on behalf of the business associate.''[17]

The Omnibus Rule defines a subcontractor as any person or entity ''delegated a function, activity, or service the business associate has agreed to perform for a covered entity or business associate.''[18] As a result, as noted above, business associates are required to enter into business associate agreements with subcontractors and can face direct liability for the failure to do so. Presumably, business associates will also face liability for failing to enter into a business associate agreement with a covered entity—an exposure that previously rested solely with the covered entity.

As has been traditionally true under the Privacy Rule structure, business associates also face contractual liability for the obligations included in a business associate agreement. In this regard the Preamble states, ''As was the case under the Privacy Rule before the HITECH Act, business associates remain contractually liable for all other Privacy Rule obligations that are included in their contracts or other arrangements with covered entities.''[19]

One of the biggest operational requirements extended to business associates is the requirement that business associates implement appropriate security measures to protect electronic PHI—security measures previously applying to covered entities and described in the Security Rule. As these are direct requirements for business associates, business associates can face direct liability for failure to meet these requirements. The Omnibus Rule provides that business associates must:

- meet the requirements of 45 C.F.R. § 164.306 related to general security requirements necessary to protect electronic PHI;
- meet the requirements of 45 C.F.R. § 164.308 related to applying appropriate administrative safeguards (including performing a risk analysis to identify potential risks and vulnerabilities to the

[14] *Id*.
[15] *Id*. at 5655.

[16] *Id*. at 5591. Those business associates that are already operating under a business associate agreement are granted a grace period to modify existing agreements. Covered entities and business associates will be deemed in compliance with the new standard if: (i) prior to January 25, 2013, the entities have entered into and are operating under a business associate agreement that has met the requirements of the Privacy Rule that were in effect on that date; and (ii) the contract or arrangement is not modified or renewed from March 26, 2013, to September 23, 2013. Such deemed compliance exists until the earlier of (i) the date the contract or arrangement is renewed or modified after September 23, 2013, or (ii) September 22, 2014. In all other cases, business associates and covered entities have until September 23, 2013, to be in compliance with the business associate requirements of the Omnibus Rule.
[17] 45 C.F.R. 160.103.
[18] 78 Fed. Reg. 5573.
[19] *Id*. at 5591-92.

confidentiality, integrity, and security of electronic PHI);

- meet the requirements of 45 C.F.R. § 164.310 related to implementing appropriate physical safeguards to protect electronic PHI;
- meet the requirements of 45 C.F.R. § 164.312 relating to implementation of appropriate technical safeguards to protect electronic PHI;
- implement appropriate organization requirements mandated by 45 C.F.R. § 164.314 to contractually obligate subcontractors to meet the above requirements; and
- develop appropriate policies and procedures to implement the requirements of the above security requirements.

Although some business associates may have anticipated this new requirement based on the HITECH Act, many may have been waiting for the implementation of regulations prior to adopting these requirements. Moreover, as noted above, because the definition of ''business associate'' includes subcontractors to business associates—all subcontractors handling electronic PHI must meet the above security requirements as well.

In sum, the changes noted above represent those changes from the Omnibus Rule that likely will have the most significant impact on covered entities and business associates.

Accordingly:

- The new breach reporting standards will need to be incorporated into policies and procedures, and, if, as expected, the new standards result in additional reporting, organizations will need to anticipate the additional costs associated with this reporting.
- Changes to the marketing rules will require not only a change to policies and procedures but a thoughtful analysis of current business relationships.
- In determining the impact of increased potential exposure for acts of business associates, covered entities and business associates will need to evaluate their business associate arrangements, assess risks and exposure, and take steps to mitigate those risks as much as possible.
- Business associates will need to undertake the time-consuming process of ensuring that all subcontractors have entered into, and understand the implications of, business associate relationships.

  HIR ISSN 2154-8986