Bloomberg BNA

BNA's
Health Law Reporter™

New HIPAA Regulations: What Liability Risks Loom Under the Expanded Business Associate and Breach Notification Provisions?

By Nancy L. Perkins

In its new omnibus final rule governing health data privacy, security, and enforcement published Jan. 25,[1] the Department of Health and Human Services has unilaterally broadened the scope of potential liability under the Health Insurance Portability and Accountability Act of 1996 to a vastly greater range of persons and entities than those Congress apparently contemplated. Confirming its view of its own authority under HIPAA, HHS adopted the expanded definition of ''business associate'' under HIPAA that it suggested in a proposed rule in 2010[2]: going forward, subcontractors of covered entities' business associates will be business associates themselves.

At the same time, HHS tightened the standards for notification of breaches of the security of health information that it prescribed in an interim final rule in 2009.[3] No longer may HIPAA covered entities and business associates determine that breach notifications are unwarranted because a data security incident appears to pose no significant risk of harm to individuals whose health information was involved. Instead, notifications are *uniformly* required unless, following an investigation, it can be determined that there is a ''low probability'' of any compromise to the security of individually identifiable health information.

These two moves—even setting aside the numerous other compliance requirements associated with the final rule—substantially raise the stakes for a wide variety of entities that may have access to medical information, particularly in light of the heightened civil and criminal penalties for data protection violations authorized by the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act.[4] Under the HITECH Act, violations of the HIPAA Privacy Rule[5] or Security Rule[6] are punishable by penalties as much as $50,000 for each violation (up to $1.5 million within a single year). In addition, state attorneys general may sue for injunctive relief, statutory damages, and attorneys' fees, with damages potentially running as high as $100 per violation or $25,000 for all violations of an

[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; Final Rule, 78 Fed. Reg. 5,566 (Jan. 25, 2013).

Nancy L. Perkins is counsel in the Washington law firm Arnold & Porter LLP. Perkins regularly advises clients on federal and state requirements for privacy and security of medical, financial, and electronic data. She has particular expertise in the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act, and their implementing regulations. She can be reached at Nancy.Perkins@aporter.com.

[2] *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40,868 (July 14, 2010).

[3] Breach Notification for Unsecured Protected Health Information, Interim Final Rule, 74 Fed. Reg. 42,740 (Aug. 24, 2009).

[4] The HITECH Act comprises Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (Feb.17, 2009).

[5] Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. Part 160 and Part 164, Subparts A and E.

[6] Standards for Security of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subpart C.

 ISSN 1064-2137

identical requirement or prohibition during a single calendar year.

Clearly, the new final rule merits close attention and counsels in favor of proactive—and timely—compliance planning. The final rule takes effect March 26 and compliance with most of its provisions is required by Sept. 23.

Background on the HITECH Act and the HIPAA Privacy and Security Rules

In the HITECH Act, Congress prescribed a number of changes to the HIPAA Privacy and Security Rules, which collectively serve to protect the privacy and security of ''protected health information'' (PHI).[7] As originally adopted by HHS, consistent with HIPAA, the Privacy and Security Rules directly applied only to HIPAA ''covered entities,'' which are (1) health plans, (2) health care clearinghouses and (3) health care providers who perform certain transactions involving health information in electronic form. The original rules affected, but did not directly apply, to business associates of those covered entities (such as billing and claims administrators, accountants, attorneys, and data management companies), by requiring that a business associate may receive an individual's PHI from a covered entity only if the covered entity obtains satisfactory assurances from the business associate that it will protect the PHI in a manner consistent with the covered entity's obligations under the Privacy Rule. Such satisfactory assurances are to be provided in a business associate agreement (BAA) between the parties that contains specific commitments.

In the HITECH Act, Congress changed this framework by making business associates *directly* liable for violation of relevant aspects of the Privacy Rule and the Security Rule. And, in an important step to help protect individuals from the adverse consequences of breaches of the security of their PHI, Congress also required HHS to adopt regulations requiring notification to individuals and HHS (and in certain cases, the media) of such breaches. Under the HITECH Act, covered entities bear the obligation to notify individuals and HHS; business associates must notify the covered entities from or on behalf of whom the business associate received the affected PHI.

What Has HHS Now Done With the ''Business Associate'' Definition?

Despite receiving many objections, HHS adopted in the final rule its proposed expansion of the HIPAA rules' definition of business associate to include *subcontractors* of HIPAA business associates. HHS acknowledged that the proposed expansion was viewed by many as ''not the intent of Congress and beyond the statutory authority of the Department,'' and that commenters believed ''creating direct liability for subcontractors will discourage such entities from operating and participating in the health care industry.''[8] But HHS disagreed, noting that the HITECH Act ''does not bar the Department from modifying definitions of terms in the HIPAA Rules to which the Act refers,'' and opining that the statute ''expressly contemplates that modifications to the terms may be necessary to carry out the provisions of the Act or for other purposes.''[9]

According to HHS, its expanded business associate definition is necessary to prevent the lapse in protection for PHI once a subcontractor is enlisted to assist a primary business associate. Thus, under the final rule, ''covered entities must ensure that they obtain satisfactory assurances required by the [HIPAA] Rules from their business associates, and business associates must do the same with regard to subcontractors, and so on, no matter how far 'down the chain' the information flows.''[10] And, as HHS further explained, the factors that determine whether a first-tier contractor is a business associate also govern the determination of whether a subcontractor is a business associate.

Who IS and Who Is NOT a Business Associate?

HHS received a number of comments objecting to the proposed expanded definition of business associate on the ground that it was confusing and ambiguous. As these comments emphasized, the ability to determine which entities are covered by the definition is critical, particularly in light of the enhanced penalties authorized by the HITECH Act. In response, HHS provided some further clarification and guidance on the scope of the new business associate definition. However, ambiguities remain.

The final rule leaves intact the basic concept of who is a business associate—*i.e.*, a person (individual or entity) who, other than as a member of the workforce of a particular covered entity,[11] performs health care functions ''on behalf of such covered entity,'' or provides certain services for the covered entity, in circumstances requiring access to PHI.[12] Thus, when a person acts on its *own* behalf, or on behalf of another person other than a particular covered entity, and does not perform any of the specified services *for* the covered entity, the person is not a business associate of that covered entity.

The same principles apply under the final rule with respect to subcontractors of business associates. The final rule defines a subcontractor as ''a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.''[13] Where the function, activity, or service the business associate has agreed to perform involves the creation, receipt, maintenance, or transmission of PHI, the subcontractor is itself a business associate and thereby directly liable for violations of the Privacy Rule, Security Rule, and Breach Notification Rule.

---

[7] PHI includes, with very narrow exceptions, any individually identifiable health information that is created or received by a health care provider, health plan, or health care clearinghouse. 45 C.F.R. § 160.103.

[8] 78 Fed. Reg. at 5,573.

[9] *Id.*

[10] *Id.* at 5,574.

[11] The ''workforce'' of a covered entity includes 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.'' 45 C.F.R. § 160.103. (Under the final rule, the same definition also covers the workforce of a business associate. *See* 78 Fed. Reg. at 5,689 (to be codified at 45 C.F.R. § 160.103).)

[12] 45 C.F.R. § 160.103. The types of services provided by a business associate are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services. *Id*.

[13] 78 Fed. Reg. at 5,689 (to be codified at 45 C.F.R. § 160.103).

  HLR ISSN 1064-2137

Importantly, as HHS has emphasized, ''[t]he final rule establishes that a person becomes a business associate by definition, not by the act of contracting with a covered entity or otherwise.[14] Thus, whether an entity is a business associate does *not depend on the existence of a BAA*.[15] The definition applies based solely on the *functional relationship* between a covered entity/business associate and another party. Therefore, a party may become a business associate even if the covered entity/business associate for whom it agrees to perform covered functions or services never mentions HIPAA, its implementing regulations, or the need for a BAA. That is true despite the obligation of each covered entity (and now each business associate) to enter into BAAs with its business associates. Even if that obligation is ignored, a party that meets the business associate definition by virtue of its functional relationship to a covered entity or business associate, is itself a business associate.

The possibility of being a business associate without the existence of a BAA suggests the need for all entities to be proactive about determining their own business associate status. For example, a document shredder hired by a covered entity/business associate to dispose of documents may or may not be a business associate, depending on whether the documents to be disposed of contain PHI. If they do, the entity is a business associate; if they do not, the entity is not a business associate.[16] Although the Privacy Rule requires a BAA to be executed if the documents do contain PHI, the covered entity's (or primary business associate's) failure to attend to that requirement will not relieve the shredding company from potential liability under the HIPAA rules. Rather, ''liability for impermissible uses and disclosures attaches immediately when a person creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate.''[17] Organizations handling PHI therefore should carefully examine their relationships with covered entities and/or business associates to assess whether any of those relationships make them business associates. Lack of vigilance in this regard could lead to serious unanticipated liability under the Privacy Rule, Security Rule, and Breach Notification Rule (discussed further below).

When Is an Entity Deemed Liable for the Acts of Its Business Associate?

Another area in which the final rule heightens potential liability with respect to business associates involves the legal principle of agency, under which the conduct of an ''agent'' is deemed attributable to the principal on whose behalf the agent acts. Although in general, covered entities are not liable for the acts of their business associates, a covered entity is liable, ''in accordance with the federal common law of agency, for a violation based on the act or omission of any agent of the covered entity.[18] However, prior to the final rule, there was an exception for business associates who are ''agents.'' Specifically, a covered entity was *not* deemed liable for the wrongful acts or omissions of business associate that is its agent, if (1) there was a HIPAA-compliant BAA in place with the business associate; (2) the covered entity did not know of a ''pattern of activity or practice'' of the business associate inconsistent with the BAA; and (3) the covered entity took ''reasonable steps'' to cure the business associate's wrongful acts or omissions and if necessary, to terminate the BAA or report the breach to HHS.[19]

The final rule eliminates this BAA exception. Under the final rule, a covered entity will be liable for the HIPAA rule violations of its business associate agents *regardless of whether there is a compliant BAA with those agents*. According to HHS, this change serves ''to ensure, where a covered entity or business associate has delegated out an obligation under the HIPAA Rules, that the covered entity or business associate would remain liable for penalties for the failure of its business associate agent to perform the obligation on the covered entity or business associate's behalf.''[20]

As indicated by the comments filed with HHS on the proposed rule, many covered entities and business associates are understandably concerned about their potential liability under an ''agency'' theory. HHS, while firmly rejecting the notion that it should abandon the agency liability doctrine in the final rule, did make an effort to provide further guidance to covered entities and business associates in determining where agency relationships exist.

As HHS noted, it is well understood that the ''terms, statements, or labels given to parties (e.g., independent contractor) do not control whether an agency relationship exists.''[21] Rather, it is the existence of actual authority of one party over another that establishes agency. More specifically, according to HHS, ''[t]he essential factor in determining whether an agency relationship exists between a covered entity and its business associate . . . is the right or authority of a covered entity to *control the business associate's conduct in the course of performing a service on behalf of the covered entity*.''[22] The same is true in determining whether an agency relationship exists between a business associate and its business associate subcontractor. Accordingly, although every situation needs to be considered on a fact-specific basis, taking into account the particular circumstances involved in the relationship between the parties, identifying the existence of an agency relationship generally requires analyzing whether the covered entity (or prime business associate) has authority to ''give interim instructions or directions'' regarding the conduct of the business associate during its performance of delegated work.[23]

---

[14] *Id.* at 5,598.
[15] *Id.* at 5,572, 5,574, 5,580.
[16] *Id.* at 5,574.
[17] *Id.* at 5,598.
[18] 45 C.F.R. § 160.402(c). In general, when a business associate is an ''agent'' of the covered entity, the covered entity is deemed liable for the business associate's failures to protect PHI, just as it is deemed liable for such failures by members of the covered entity's own workforce.
[19] *Id.*
[20] 78 Fed. Reg. at 5,580.
[21] *Id.* at 5,581.
[22] *Id.*
[23] *Id.* Other key factors that bear on the analysis include (1) the time, place, and purpose of a business associate agent's conduct; (2) whether a business associate agent engaged in a course of conduct subject to a covered entity's control; (3) whether a business associate agent's conduct is commonly done by a business associate to accomplish the service performed on behalf of a covered entity; and (4) whether or not

Frequently, a key indicator of such authority is the written contract (if any) between the parties. In general, the more specific the contract is in setting forth the respective obligations of the parties, the less likely that it establishes an agency relationship. For example, a business associate generally would not be an agent if it enters into an agreement with a covered entity that sets forth very clearly the terms and conditions of the business associate's performance, leaving the covered entity with no ability to control that performance, other than through an amendment of the terms of the agreement or by suing for breach of contract. On the other hand, if the parties' agreement authorizes the covered entity to direct the performance of the service provided by its business associate during the course of the relationship, the business associate likely is the covered entity's agent.[24]

These principles have important implications for BAAs under the Privacy and Security Rules. Often, covered entities seek to maintain flexibility to decide, on a case-by-case basis, how their business associates will fulfill their BAA obligations, such as the obligation to either make PHI available for amendment or, rather, to simply amend the PHI. A BAA might state, for example, that the ''business associate must make available protected health information based on the instructions to be provided by or under the direction of a covered entity.''[25] According to HHS, such a statement would indicate that the business associate is an agent of the covered entity, ''because the covered entity has a right to give interim instructions and direction during the course of the relationship.''[26]

This suggests that covered entities—and business associates with respect to subcontractors—should consider how their BAAs may affect their own liability for the acts of their business associates. Although limiting such liability may entail sacrificing some control over a business associate, the benefits could be substantial, particularly with respect to potential violations of the Breach Notification Rule (discussed further below). In general, covered entities and business associates should undertake to identify, based on all relevant facts and with the advice of legal counsel, which, if any, of their business associates are their ''agents.'' Accurately making such determinations, and implementing procedures to ensure adequate supervision and monitoring of agents, will be a critical, ongoing process for HIPAA covered entities and business associates.

Must BAAs Be Amended Under the Final Rule?

Although, as noted, the existence of a BAA is not determinative of whether a ''business associate'' relationship exists, the final rule nevertheless explicitly requires BAAs. In accordance with the HITECH Act, all BAAs must incorporate the new privacy and security obligations established the act, including the security breach notification requirements. And, by extending the business associate definition to qualifying subcontractors of business associates, the final rule mandates BAAs not only for covered entities' business associates, but also for subcontractor business associates, as well as sub-subcontractor business associates, sub-sub-business associates, etc. This will be a new endeavor with respect to many subcontractors, because although it has been a business associate's obligation to ''[e]nsure that any agents, including a subcontractor, to whom it provides protected health information . . . agrees to the same restrictions and conditions that apply to the business associate with respect to such information,''[27] HHS has not previously required a subcontractor *BAA*—or even a *written* agreement at all. Now, the final rule requires all business associates to execute HIPAA-compliant BAAs. (A covered entity, however, is not responsible for entering into any BAAs with its business associates' subcontractors, nor is any business associate required to enter into BAAs with the subcontractors of its business associates.)[28]

To assist covered entities and business associates in ensuring that their BAAs contain all the required clauses, HHS has posted sample BAA clauses on its website.[29] Although these sample clauses are somewhat helpful, it will be a major task for the thousands of entities that now qualify as business associates to execute the required BAAs.

Recognizing the magnitude of this task, HHS has provided an extended timetable for the execution of fully compliant BAAs. Rather than requiring that this be done by the final rule's general compliance date of Sept. 23, HHS is giving covered entities and business associates staggered deadlines, depending on whether there is an existing BAA. Specifically, the final rule provides that any BAA that (i) complies with the current Privacy and Security Rules, (ii) was entered into prior to Jan. 25 (the publication date of the final rule), and (iii) is not renewed or modified between March 26 (the final rule's effective date) and Sept. 23 (the final rule's general compliance date), will be deemed in compliance with the final rule until the earlier of:

1. the date the BAA is renewed or modified on or after Sept. 23, 2013, and
2. Sept. 22, 2014.

Essentially, this means that, absent any reworking of a preexisting, currently compliant BAA, the BAA will be deemed in compliance with the final rule for a full year after the final rule's general compliance date.

New Risks Under the Breach Notification Rule: What Triggers the Notification Requirements?

As noted, HHS adopted the Breach Notification Rule in 2009 as interim final rule and invited comment while commencing enforcement. The final rule reflects HHS's consideration of the comments it received, but largely leaves the 2009 version intact—with one significant exception. Whereas the interim rule provided that notifications of security incidents involving PHI were required *only* if there was evidence of a ''significant risk of harm'' to individuals from the incident, the final rule requires notification *unless* the covered entity or business associate, as applicable, ''demonstrates that there is a low probability that the protected health informa-

---

the covered entity reasonably expected that a business associate agent would engage in the conduct in question. *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] 45 C.F.R. § 164.50(e)(ii)(D).

[28] *See* 78 Fed. Reg. at 5573.

[29] *See* Dep't of Health & Human Services, Health Information Privacy, Sample Business Associate Agreement Provisions (Jan. 25, 2013), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

  HLR ISSN 1064-2137

tion has been compromised.''[30] Thus, the final rule creates a presumption in favor of notification, and places the burden of proof on the covered entity/business associate to overcome that presumption.

The Interim Rule and Reactions to It

The Breach Notification Rule applies to any ''unsecured'' protected health information (PHI), which means any individually identifiable health information that is unsecured. Electronic PHI is unsecured under the rule if it is neither properly encrypted nor destroyed. Any other form of PHI is unsecured unless it is destroyed.[31] For many HIPAA covered entities and business associates, it is not feasible to encrypt all the PHI they maintain, and thus they must be prepared to respond to a data security breach in compliance with the Breach Notification Rule.

The trigger for the application of the HHS breach notification requirements is a breach of data security. With three limited exceptions, the interim rule defined a breach of the security of PHI as ''the acquisition, access, use, or disclosure'' of PHI not permitted under the Privacy Rule ''which compromises the security or privacy'' of the PHI.[32] As clarification of that definition, the Interim Rule provided that the phrase ''compromises the security or privacy'' of an individual's PHI means ''poses a significant risk of financial, reputational, or other harm to the individual.''[33]

The ''risk of harm'' standard in the interim rule drew sharp criticism, including from members of Congress. In a formal comment letter on the interim rule, six representatives asserted that the HITECH Act ''does not imply a harm standard.''[34] According to these representatives, when the HITECH Act was being drafted, House members ''specifically considered and rejected such a standard,'' and instead ''passed legislation that has a black and white standard for notification.'' The members urged HHS ''to revise or repeal the harm standard provision included in its interim final rule at the soonest appropriate opportunity.''

Similar views were expressed by certain privacy advocates.[35] Members of the health care industry, in contrast, strongly supported the risk-of-harm standard, noting that such a standard has been endorsed by numerous state legislatures in their own their breach notification laws. Industry members also argued that the standard serves consumer's interests by preventing unnecessary and unwarranted anxiety to individuals caused by notifications of breaches that actually pose little or no risk of harm, as well as potential apathy among consumers if such notifications are frequently sent.[36]

The Final Rule's Changes

In response to the criticisms of the ''risk of harm'' standard, while recognizing the points made in support of such a standard, HHS replaced the risk of harm component of the breach definition in the final rule with the new presumption in favor of notification. HHS explained its reasons for the change as follows:

> We believe that the express statement of this presumption in the final rule will help ensure that all covered entities and business associates interpret and apply the regulation in a uniform manner and also [that it] responds to commenters that indicated the default function of the rule was unclear. . . . [W]e have removed the harm standard and modified the risk assessment to focus more objectively on the risk that the protected health information has been compromised. . . . The final rule . . . identifies the more objective factors covered entities and business associates must consider when performing a risk assessment to determine if the protected health information has been compromised and breach notification is necessary.[37]

The ''objective factors'' referred to by HHS consist of particular situational circumstances that, in HHS's view, can demonstrate that there is a low probability that PHI information has been compromised. Specifically, under the final rule, covered entities and business associates must conduct a risk assessment that analyzes:

> (1) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
>
> (2) the unauthorized person who used the protected health information or to whom the disclosure was made;
>
> (3) whether the protected health information actually was acquired or viewed; and
>
> (4) the extent to which the risk to the protected health information has been mitigated.[38]

A covered entity or business associate must address each of these factors in analyzing the probability that PHI has been compromised by a security incident, although other factors may be considered as well. The re-

[30] 78 Fed. Reg. at 5,695 (to be codified at 45 C.F.R. § 164.402).

[31] As specified in guidance posted on the HHS website, to be properly *encrypted*, the information must have been transformed, through the use of an algorithmic process, ''into a form in which there is a low probability of assigning meaning without use of a confidential process or key,'' and such process or key has not been breached. The encryption methods verified by the National Institute of Standards and Technology meet this standard. Dep't of Health & Human Services, Health Information Privacy, Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

[32] 45 C.F.R. § 164.402. The three exceptions to the breach definition are narrow. They apply when: (1) PHI is unintentionally accessed, acquired, or used by a member of the workforce of a HIPAA covered entity or business associate in a work-related context and in good faith, where there is no further use or disclosure of the PHI; (2) PHI is inadvertently disclosed by one individual who rightfully has access to the PHI to another individual at the same covered entity, business associate, or organized health care arrangement who also has the right to access PHI, as long as there is no further use or disclosure of the PHI; or (3) PHI is disclosed by a covered entity or business associate to an unauthorized person but the covered entity or business associate has a ''good faith belief'' that such person would not reasonably have been able to retain the PHI. *Id.*

[33] *Id.*

[34] Letter from Reps. Henry Waxman, John Dingell, Joe Barton, Frank Pallone, Charles Rangel, and Pete Stark to Health and Human Services Secretary Kathryn Sebelius (Oct. 1, 2009), http://op.bna.com/hl.nsf/r?Open=psts-954l5v.

[35] 78 Fed. Reg. at 5,641.

[36] *Id.* at 5,640-41.

[37] *Id.* at 5,641-42.

[38] 78 Fed. Reg. at 5695 (to be codified at 45 C.F.R. § 164.402).

quired assessment should consider all factors in combination, and HHS ''expect[s] these risk assessments to be thorough, completed in good faith, and for the conclusions reached to be reasonable.''[39]

The types of considerations relevant to the four factors that must be addressed include:

1. What type and amount of PHI was subject to disclosure? For example, was it just a list of a dentists' charges to a particular medical account number? Or was it a record of an abortion or a prescription for AIDs medication? In the former case, it likely would be reasonable to conclude that there is low probability that the 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. In contrast, in the latter case, such a conclusion likely would not be reasonable.
2. Who impermissibly used or accessed the PHI? Does the Privacy Rule or Security Rule, or any similar statutory or regulatory protections for data privacy, apply to the unauthorized recipient? If so, there may be a lower probability that the protected health information has been compromised, since the recipient is required to keep the information confidential and protect its security.
3. Was the PHI returned before there was an opportunity for it to be actually acquired or viewed? For example if the PHI was in a file stored on a laptop computer that was lost or stolen but then recovered, and a forensic analysis shows that file was not opened or transferred, the probability of compromise of the PHI is low. In contrast, if a fax containing PHI went to the wrong patient, there would be a higher probability of misuse.
4. Were steps taken to mitigate risk of harm, such as obtaining satisfactory assurances from the unauthorized recipient of PHI that the PHI will not be retained or further used or disclosed? If a written confidentiality agreement is obtained that provides commitments to that effect, for example, it may be reasonable to conclude that there is a low probability that the PHI was compromised.

A thorough assessment of these factors must be done in any case of a suspected breach (unless a decision is made to proceed with the notifications in any event). Because covered entities and business associates have the burden of proof to demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach, it is critical to document the basis for determinations that notifications were not required, such as in memoranda and reports, including forensic evidence. If any such determination is called into question in an investigation or administrative proceeding, this documentation will be essential to defend the decision not to provide notifications.

Implications of Business Associate Relationships for Breach Notifications

As noted, HHS did not alter the basic requirements of the Breach Notification Rule, other than the ''risk of harm'' standard, in the final rule. However, HHS did clarify and underscore how important it is for covered entities and business associates (now including business associate subcontractors) to delineate clearly the responsibilities of a business associate, and in particular business associates acting as agents, to mitigate potential liability under the Breach Notification Rule.

As has previously been required, under the final rule, a covered entity must provide breach notifications to individuals without ''unreasonable delay'' and in any event within 60 days of the date of discovering the breach. The same time constraint applies to the notifications business associates must provide to covered entities upon discovery of a security breach. In both cases, a breach is deemed ''discovered'' by the covered entity/business associate on the date that any member of the workforce, or *any agent,* of the covered entity/business associate discovers the breach. Discovery of a breach occurs at the time the breach is first known *or, ''by exercising reasonable diligence would have been known,''* to the discovering entity.[40] ''Reasonable diligence'' means the ''business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.''[41]

Because the discovery of a breach by a business associate acting as an agent of a covered entity is imputed to the covered entity, the covered entity must provide notifications within 60 days after the date when such a business associate *discovers* the breach, not 60 days after the date when the business associate *notifies* the covered entity of the breach. Under the final rule, the same time constraint governs notifications that must be made by business associates with respect to breaches discovered by their subcontractor business associates acting as agents.

In comments submitted to HHS on the interim rule, objections were made to the requirement that breach notifications be provided within 60 days after a data security incident is first *discovered*, as opposed to 60 days after it is determined, based on an investigation and analysis, that the incident actually constitutes a breach.[42] These comments argued that 60 days is an insufficient amount of time to conduct a thorough investigation and analysis and also prepare all the documentation needed to provide proper notifications, particularly where the number of affected individuals is very large. They therefore advocated that the 60-day clock should not start to tick upon discovery of a breach, but, rather, when it has been *determined that a breach occurred*.[43] HHS summarily rejected this proposal. According to HHS, ''[t]here is sufficient time within this standard both to conduct a prompt investigation of the incident and to notify affected individuals.''[44]

The final rule's retention of the maximum 60-day notification period, coupled with the new presumption in favor of notification, underscores the importance of properly managed business associate relationships, particularly those involving business associates acting as agents. HHS alluded to this in issuing the final rule, stating that ''[b]ecause of the agency implications on the timing of breach notifications, we encourage covered entities to discuss and define in their business associate agreements the requirements regarding how,

[39] *Id.* at 5,643.

[40] 45 C.F.R. § § 164.404(a)(2), 164.410(a)(2) (emphasis added).

[41] *Id.* § 160.410(a).

[42] 78 Fed. Reg. at 5,648.

[43] *Id.*

[44] *Id.*

  HLR ISSN 1064-2137

when, and to whom a business associate should notify the covered entity of a potential breach.''[45]

To properly address the timing for breach notifications in their BAAs, covered entities, as well as business associates with respect to their subcontractors, need to determine, with the assistance of legal counsel, which of their business associates qualify as agents. This determination can help inform (and in fact be driven by, as discussed above regarding the indicia of agency), appropriate language in BAAs. If a covered entity seeks to ensure that one or more of its business associates will *not* be deemed its agent—which will mean the business associate's discovery of a breach will not be imputed to the covered entity—it should include in the BAA, as well as any underlying services agreement with the business associate, as much specificity as possible regarding the business associate's obligations. For example, the BAA could state, with respect to breach notifications, that the business associate ''shall notify the covered entity within three business days of any known or suspected breach involving PHI'' and specify that such notification include a report on the date and time of the breach, the type and amount of PHI affected, the known facts of how the breach occurred and whether and how it has been addressed, and a description of all steps being taken to mitigate any harm to individuals from the breach. These types of specific requirements will help in both defining the nature of the relationship between the parties (*i.e.*, whether it involves agency) and in ensuring that they will be able to responsibly and effectively fulfill their obligations under the omnibus final rule.

[45] *Id.* at 5656.