MINIMIZING LIABILITY FOR BUSINESS ASSOCIATE MISCONDUCT

By Kim C. Stanger

Republished with permission from AHLA's Physicians and Hospitals Law Institute. Original article appeared Feb. 5, 2018.

Healthcare providers, health plans and healthcare clearinghouses ("covered entities") and business associates are subject to significant penalties for violations of the HIPAA Privacy, Security and Breach Notification Rules. To make matters worse, covered entities may be liable for their business associates' misconduct, and business associates may be liable for their subcontractors' violations. Covered entities and business associates must take appropriate steps to minimize exposure for their business associates' or subcontractors' violations.

1. HIPAA CIVIL PENALTIES. The civil penalties for HIPAA violations were recently increased as summarized in the following chart:

Conduct of covered entity or business associate	**Penalty**
Did not know and, by exercising reasonable diligence, would not have known of the violation	$112 to $55,910 per violation; Up to $1,667,299 per identical violation per year
Violation due to reasonable cause and not willful neglect	$1,118 to $55,910 per violation; Up to $1,667,299 per identical violation per year
Violation due to willful neglect but the violation is corrected within 30 days after the covered entity knew or should have known of the violation	Mandatory fine of $11,182 to $55,910 per violation; Up to $1,667,299 per identical violation per year
Violation due to willful neglect and the violation was not corrected within 30 days after the covered entity knew or should have known of the violation	Mandatory fine of not less than $55,910 per violation; Up to $1,667,299 per identical violation per year

As reflected in the chart, HIPAA penalties are mandatory if a covered entity or business associate acts with willful neglect. On the other hand, a covered entity or business associate who does not act with willful neglect and who corrects the violation within thirty (30) days may avoid HIPAA penalties; correcting the situation is an affirmative defense to penalties. (45 CFR § 160.402).

2. LIABILITY FOR BUSINESS ASSOCIATE OR SUBCONTRACTOR MISCONDUCT. Under HIPAA, covered entities and business associates may be liable for their business associates' and subcontractors' violations in the following circumstances:

2.1 Knowing of But Failing to Stop Misconduct. Per the HIPAA Privacy Rule,

> (ii) A covered entity is not in compliance with [HIPAA] if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

> (iii) A business associate is not in compliance with [HIPAA], if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(45 CFR § 164.504(e)(1)). While covered entities and business associates are not required to actively monitor their business associates or subcontractors, they must act promptly to address any violation of which they become aware. HHS explained:

> we will view a covered entity that has substantial and credible evidence of a violation as knowing of such violation. While this standard relieves the covered entity of the need to actively monitor its business associates, a covered entity nonetheless is expected to investigate when they receive complaints or other information that contain substantial and credible evidence of violations by a business associate, and it must act upon any knowledge of such violation that it possesses.

(65 FR 82505; *see also id.* at 82641). Thus, "[c]overed entities cannot avoid responsibility by intentionally ignoring problems with their contractors. (65 FR 82505).

2.2 Business Associate as Agent. Under HIPAA, covered entities and business associates may be vicariously liable for penalties imposed against their agents:

> *Violation attributed to a covered entity or business associate.*
>
> (1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.
>
> (2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

(45 CFR § 160.402(c)). The Omnibus Rule contains a fairly extensive discussion of factors that may establish an agency relationship. According to HHS,

> An analysis of whether a business associate is an agent will be fact specific, taking into account the terms of a business associate agreement as well as the totality of the circumstances involved in the ongoing relationship between the parties. The essential factor in determining whether an agency relationship exists between a covered entity and its business associate (or business associate and its subcontractor) 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. The right or authority to control the business associate's conduct also is the essential factor in determining whether an

> agency relationship exists between a business associate and its business associate subcontractor.

(78 FR 5581, emphasis added). In making that determination,

> 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.

(78 FR 5581). The analysis "will be fact specific and consider the totality of the circumstances involved in the ongoing relationship between the parties." (78 FR 5581). HHS also noted that

> a business associate can be an agent of a covered entity: (1) Despite the fact that a covered entity does not retain the right or authority to control every aspect of its business associate's activities; (2) even if a covered entity does not exercise the right of control but evidence exists that it holds the authority to exercise that right; and (3) even if a covered entity and its business associate are separated by physical distance (e.g., if a covered entity and business associate are located in different countries).

(78 FR 5581).

2.2.1 Factors Evidencing Agency. Although not exclusive, HHS identified certain factors that may evidence an agency relationship:

2.2.1.1 The ability to give interim instructions. According to HHS:

> The authority of a covered entity to give interim instructions or directions is the type of control that distinguishes covered entities in agency relationships from those in non-agency relationships. A business associate generally would not be an agent if it enters into a business associate agreement with a covered entity that sets terms and conditions that create contractual obligations between the two parties. Specifically, if the only avenue of control is for a covered entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a business associate is not acting as an agent. In contrast, a business associate generally would be an agent if it enters into a business associate agreement with a covered entity that granted the covered entity the authority to direct the performance of the service provided by its business associate after the relationship was established. For example, if the terms of a business associate agreement between a covered entity and its business associate stated that ''a business associate must make available protected health information in accordance with § 164.524 based on the instructions to be provided by or under the direction of a covered entity,"' then this would create an agency relationship between the covered entity and business associate for this activity because the covered entity has a right to give interim instructions and direction during the course of the relationship.

(78 FR 5581).

2.2.1.2 Delegation of a required function. The delegation of a required function may establish agency or otherwise subject the covered entity to liability if the business associate fails to comply with rules relating to that function. HHS explained:

> An agency relationship also could exist between a covered entity and its business associate if a covered entity contracts out or delegates a particular obligation under the HIPAA Rules to its business associate…. [W]hether or not an agency relationship exists in this circumstance again would depend on the right or authority to control the business associate's conduct in the performance of the delegated service based on the right of a covered entity to give interim instructions.

(78 FR 5581).

2.2.1.3 The nature of the services provided by the business associate. According to HHS:

> The type of service and skill level required to perform the service are relevant factors in determining whether a business associate is an agent. For example, a business associate that is hired to perform de-identification of protected health information for a small provider would likely not be an agent because the small provider likely would not have the expertise to provide interim instructions regarding this activity to the business associate.

(78 FR 5581).

2.2.1.4 Whether the covered entity is prohibited from providing the service. Whether the covered entity may perform the service assigned to the business associate is another factor to consider:

> an agency relationship would not likely exist when a covered entity is legally or otherwise prevented from performing the service or activity performed by its business associate. For example, the accreditation functions performed by a business associate cannot be performed by a covered entity seeking accreditation because a covered entity cannot perform an accreditation survey or award accreditation

(78 FR 5581-82).

2.2.1.5 Other factors. In an oft-cited decision, the Supreme Court identified additional relevant factors that may be helpful in applying the federal common law of agency:

> In determining whether a hired party is an employee under the general common law of agency, we consider [1] the hiring party's right to control the manner and means by which the product is accomplished. Among the other factors relevant to this inquiry are [2] the skill required; [3] the source of the instrumentalities and tools; [4] the location of the work; [5] the duration of the relationship between the parties; [6] whether the hiring party has the right to assign additional projects to the hired party; [7] the extent of the hired party's discretion over when and how long to work; [8] the method of payment; [9] the hired party's role in hiring and paying assistants; [9] whether the work is part of the regular business of the hiring party; [10] whether the hiring party is in

> business; [11] the provision of employee benefits; and [11] the tax treatment of the hired party. See Restatement [(Second) of Agency] § 220(2) (setting forth a nonexhaustive list of factors relevant to determining whether a hired party is an employee). No one of these factors is determinative.

(*Community for Creative Non-Violence v. Reid*, 490 U.S. 730, 750 (1989)).

2.2.2 Scope of Agency. Even if an agency relationship exists, covered entities and business associates are only vicariously liable for their agents' acts within the scope of their agency. (78 FR 5582; *see also* 45 CFR § 160.402(c)). According to HHS,

> Several factors are important to consider in any analysis to determine the scope of agency: (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 the covered entity reasonably expected that a business associate agent would engage in the conduct in question.

(78 FR 5581). Deviation from the terms of a business associate agreement ("BAA") does not necessarily mean that the business associate was acting outside the scope of his agency:

> A business associate agent's conduct generally is within the scope of agency when its conduct occurs during the performance of the assigned work or incident to such work, regardless of whether the work was done carelessly, a mistake was made in the performance or the business associate disregarded a covered entity's specific instruction. For example, a business associate agent would likely be acting within the scope of agency if it impermissibly disclosed more than the minimum necessary information to a health plan for purposes of payment, even if the disclosure is contrary to clear instructions of the covered entity. In contrast, a business associate agent's conduct generally is outside the scope of agency when its conduct is solely for its own benefit (or that of a third party), or pursues a course of conduct not intended to serve any purpose of the covered entity.

(78 FR 5582).

2.2.3 Knowledge of the Agent. The existence of an agency relationship may also affect relevant deadlines for HIPAA compliance. For example, knowledge of a business associate who is an agent may be imputed to the principal for purposes of triggering the obligation to respond to violations; the 30-day deadline for correcting violations and avoiding penalties; and/or the 60-day period for reporting breaches. (*See* 78 FR 5647; *see also* 78 FR 5655). Nevertheless, HHS has indicated that an agent's knowledge is not imputed to the principal if (1) the agent consciously acts in a manner that is adverse to the principal (75 FR 40879), or (2) the agent acts outside the scope of agency by, *e.g.*, failing to notify the covered entity of a violation. (78 FR 5587).

The knowledge of the agent may also be relevant in determining the covered entity's *mens rea* for calculating HIPAA's tiered penalties. HHS explained:

> in some circumstances, we expect that the knowledge of an employee or agent of a covered entity or business associate may determine whether a violation implicates the ''did not know'' or ''reasonable cause'' categories of violation. That is, absent an exception under the Federal common law of agency, the knowledge of an employee or agent will generally be imputed to its principal (i.e., the covered entity or business associate). See 70 FR 20224, 20237 and 71 FR 8390, 8402–3 (discussing imputation of knowledge under the Federal common law of agency and violations attributed to a covered entity, respectively). Consider the following example:
>
> A hospital employee accessed the paper medical record of his ex-spouse while he was on duty to discover her current address for a personal reason, knowing that such access is not permitted by the Privacy Rule and contrary to the policies and procedures of the hospital. HHS's investigation reveals that the covered entity had appropriate and reasonable safeguards regarding employee access to medical records, and that it had delivered appropriate training to the employee.
>
> In this example, the ''did not know'' category of violation is implicated with respect to the covered entity because the *mens rea* element of knowledge cannot be established. That is, while the employee's act is attributed to the covered entity, the employee's knowledge of the violation cannot be imputed to the covered entity because the employee was acting adversely to the covered entity. The Federal common law of agency does not permit the imputation of knowledge to the principal where the agent consciously acts in a manner that is adverse to the principal.

(75 FR 40878-79). HHS's analysis suggests that a covered entity may avoid mandatory "willful neglect" penalties despite the intentional misconduct of its agents so long as the covered entity establishes that the agent was acting outside the scope of his or her authority, *e.g.*, the agent was acting in a manner adverse to the covered entity.

2.3 Delegated Duties. HIPAA requires that BAAs contain required terms. Under the Omnibus Rule, "[t]o the extent the business associate is to carry out a covered entity's obligation" required by the HIPAA Privacy Rule, the BAA must require business associates to "comply with the requirements of [the HIPAA Privacy Rule] that apply to the covered entity in the performance of such obligation." (45 CFR § 164.504(e)(2)(ii)(H)). The Omnibus Rule commentary states:

> where a covered entity or business associate has delegated out an obligation under the HIPAA Rules, … a 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.

(78 FR 5580). In addition, as discussed above, delegating such duties may also suggest that the BA is acting as the agent of the covered entity. (78 FR 5581). BAAs often delegate certain tasks to business associates or subcontractors, *e.g.*, providing individuals with access to PHI; amending PHI; accounting for disclosures of PHI; and breach notification. Service agreements may delegate other duties, including implementation of IT security, record maintenance or destruction, etc. By delegating such functions, covered entities are opening themselves to potential liability for the business associate's mistakes. Business associates and subcontractors may not understand relevant HIPAA obligations; covered entities may need to ensure that business associates and subcontractors understand their responsibilities if they are to perform delegated tasks for the covered entity.

2.4 Failure to Execute BAA. According to HHS, "[i]f a covered entity fails to comply with the business associate provisions in the Privacy and Security Rules, such as by not entering into the requisite contracts or arrangements …, the covered entity may be liable for the actions of a business associate agent." (71 FR 8403). Over the past year, the OCR has settled several cases against covered entities based in whole or in part on their failure to obtain BAAs before disclosing PHI to their business associates. For example:

In March 2016, North Memorial Health Care of Minnesota agreed to pay $1.55 million to settle OCR charges that it violated HIPAA by disclosing PHI to its business associate, Accretive Health, without first executing a BAA. The issue surfaced following the theft of an Accretive employee's unencrypted, password-protected laptop containing PHI of approximately 9,500 individuals. Note that it was the business associate's laptop that was lost, not the covered entity's; nevertheless, the OCR extracted the settlement from the covered entity. The OCR also cited North Memorial's failure to conduct an appropriate risk analysis. For a copy of the press release, *see* https://archive-it.org/collections/3926?fc=meta_Date:2016.

In April 2016, Raleigh Orthopedic Clinic agreed to pay $750,000 to settle OCR allegations that it violated HIPAA by turning over thousands of x-rays and related protected health information to a vendor without a BAA. The vendor had promised to transfer the x-rays to electronic media in exchange for salvaging silver from the x-ray films. For a copy of the press release, *see* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic-bulletin/index.html. In its press release, the OCR reaffirmed,

> HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise. It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected.

Id.

The failure to obtain BAAs is clearly a violation of the HIPAA Privacy and Security Rules. Nevertheless, these cases are troubling for several reasons. First, there is nothing in the published agreements or press releases to suggest that the business associates were acting as the covered entities' agents so as to make the covered entities vicariously liable for the business associate's conduct per 45 CFR § 160.400; thus, the covered entities were purportedly punished for their own misconduct, which misconduct would seem to be relatively innocuous.

Second, business associates are obligated to comply with the HIPAA Security Rule and the mandatory BAA terms even if no BAA is executed (*see* 78 FR 5574); accordingly, it is difficult to understand how the absence of a written BAA caused or contributed to any resulting damages or warranted such large penalties, especially when the business associate is a sophisticated party such as Accretive Health who surely understood its HIPAA obligations.

Admittedly, we do not know all the underlying facts that triggered the OCR's response in each case; nevertheless, they serve as a sober warning that the OCR may look to covered entities to pay the price of their business associate's misconduct if there is not an appropriate BAA in place.

These cases raise another question: under the HIPAA Breach Notification Rule, must a covered entity self-report the improper disclosure of PHI to a business associate if there is no BAA? The disclosure of PHI to a business associate without a BAA is a violation of the HIPAA Privacy Rule, but not all Privacy Rule violations are reportable. A covered entity need not report an improper use, access, or disclosure if there is a low probability that the information has been compromised. (*See* 45 CFR § 164.402). In its Omnibus Rule commentary, HHS suggested that an improper disclosure to another HIPAA covered entity who is otherwise obligated to maintain the confidentiality of the information may indicate that there is a low probability that the data has been compromised, *e.g.*, where

PHI is faxed to the wrong physician's office. (*See* 78 FR 5642). If so, then disclosure to a business associate—who is obligated to maintain the confidentiality of the information even if there is no written BAA—would seem to suggest a low probability that the data has been compromised, and, hence, the disclosure should not be reportable. Nevertheless, covered entities should carefully analyze the facts of each case given the OCR's recent decisions.

3. MINIMIZING LIABILITY FOR BUSINESS ASSOCIATE MISCONDUCT. Taking the following steps may help covered entities and business associates minimize their liability for their respective business associates' or subcontractors' misconduct:

3.1 Comply with the HIPAA Rules. Covered entities and business associates should ensure they comply with the HIPAA Privacy and Security Rules regardless of their business associate's actions; doing so will help establish that the covered entity did not act with "willful neglect", thereby allowing it to minimize or avoid penalties. Among other things, covered entities should conduct and document appropriate risk assessments; implement policies and safeguards required by the Security, Privacy and Breach Notification Rules; execute valid BAAs; train workforce members and document such training; and respond promptly to violations or breaches.

3.2 Identify Business Associates. Covered entities must identify and execute appropriate BAAs with their business associates. Business associates must identify and execute BAAs with their subcontractors. They should train their staff concerning BAA requirements, and periodically review their business associate relationships as part of their recurring risk analysis.

HIPAA defines business associates as persons who:

> (i) On behalf of such covered entity or of an organized health care arrangement … in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA],… or
>
> (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation …, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(45 CFR § 160.103, definition of "business associate"). "A covered entity may be a business associate of another covered entity" when performing business associate functions for the principal covered entity. (*Id.*). The HIPAA Omnibus Rule confirms that the following are business associates:

> (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
>
> (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

> (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(*Id.*). The Omnibus Rule significantly expanded the business associate pool by confirming that entities which "maintain" PHI are business associates even if they do not actually view the PHI, including but not limited to cloud service providers and other data storage companies:

> a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold. To help clarify this point, we have modified the definition of ''business associate'' to generally provide that a business associate includes a person who ''creates, receives, *maintains*, or transmits'' (emphasis added) protected health information on behalf of a covered entity.

(78 FR 4472). Such entities are business associates even if the PHI is encrypted and the entity does not maintain the key. (OCR FAQ dated 10/6/16).

Although by no means exhaustive, the following are some of the more common business associates if and to the extent they handle PHI as part of their job duties for the covered entity: data storage companies, including cloud service providers; data processing or management companies; document destruction companies; health information exchanges; EHR vendors; e-prescribing gateways; software vendors or IT support; vendors of equipment or services that access PHI; medical device manufacturers that access PHI; management companies; billing companies; answering services; transcription services; interpreters or translators if contracted to provide their services on behalf of the covered entity; consultants; auditors; marketing or public relations firms; accountants; lawyers; malpractice carriers; collection agencies if performing services for the covered entities; third party administrators for the provider's employee group health plan; accreditation organizations; patient safety organizations; state or national industry associations that provide services; peer reviewers who review records; medical directors or other clinicians providing administrative services unless they are members of an organized healthcare arrangement; *etc*.

3.3 Execute Appropriate BAAs. Covered entities and business associates must execute BAAs that contain at least the elements set forth in the HIPAA Privacy and Security Rules, 45 CFR §§ 164.314, 164.502(e), and 164.504(e).

3.3.1 Required terms. Among other things, the BAA must identify permitted uses and disclosures; require the BAA to comply with the Security Rule and use appropriate safeguards to protect PHI; require reports of violations, security incidents and reportable breaches; require the business associate to assist the covered entity in responding to requests by patients to access, amend, or obtain an accounting of their information; require the business associate to comply with HIPAA Rules if and to the extent the covered entity delegates required functions to the business associate; allow HHS to access the BAA's records to investigate compliance; require BAAs with subcontractors; permit termination of the BAA for noncompliance; and address the return, destruction, or protection of PHI post-termination. (45 CFR § 164.504(e)). The OCR has published sample BAA language on its website, https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

When executing BAAs, the parties should compare and coordinate the BAA with the underlying service agreement to ensure they are consistent. The services agreement may affect permissible uses and disclosures under the BAA; the parties should ensure that those uses are consistent with HIPAA and the BAA. In the event of a conflict, the BAA should control.

The parties should periodically review the BAAs to ensure they are still appropriate to the relationship and comply with applicable regulations. In 2016, a provider was required to pay $400,000 because it failed to update its BAA to comply with the 2013 Omnibus Rule requirements. (*See* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/wih).

3.3.2 Additional terms. Although not required, covered entities and business associates may want to include additional terms to help minimize their liability for their business associate's or subcontractor's misconduct. For example, the BAA should address the following:

3.3.2.1 Explain business associate duties. Business associates and subcontractors who are unsophisticated may not understand or appreciate their obligations under HIPAA. Accordingly, covered entities may want to be relatively specific when setting forth the business associate duties in the BAA, including the obligation to comply with the Security Rule, identify and respond to breaches, or account for impermissible disclosures. Alternatively, covered entities may want prepare and provide to business associates a separate letter or document that explains the business associate's obligations.

3.3.2.2 Confirm independent contractor status. The BAA as well as the underlying service agreement should confirm that the business associate or subcontractor is acting as an independent contractor and not as the agent of the covered entity. Unless the covered entity is willing to assume liability for the business associate's acts or omissions, the covered entity should be careful about delegating required functions to the business associate, or including terms that suggest the covered entity has the authority to control the method or manner of the business associate's performance, including but not limited to the right to give interim instructions.

3.3.2.3 Timely notice. Covered entities have only thirty (30) days to correct violations and avoid penalties, and sixty (60) days to report breaches of unsecured health information. The immediate response may help mitigate or avoid liability. Accordingly, the BAA should require business associates and subcontractors to promptly notify the covered entity of breaches or violations, *e.g.*, within five (5) business days.

3.3.2.4 Cooperation, indemnification and insurance. The BAA should require business associates and subcontractors to cooperate with the covered entity's response to any violation. If possible, it should require the business associate to reimburse the covered entity for its costs in responding to violations, and indemnify the covered entity against third party claims or penalties imposed because of the business associate's or subcontractor's misconduct. To ensure there is a source of payment, the covered entity may want to require the business associate and its subcontractors to carry appropriate liability insurance. Although it may be common to do so, covered entities should be careful about delegating to the business associate its obligation to respond to breaches or violations. The business associate may be tempted to minimize its role or response to avoid cost and liability. As discussed above, the covered entity may be liable if and to the extent that the business associate fails to properly perform a delegated task. The covered entity should beware provisions in the underlying service agreement that may limit or cap the business associate's obligations to cooperate, defend or indemnify the BAA.

3.3.2.5 Subcontractor liability. The BAA should ensure that the obligations imposed on the business associate are passed through to the business associate's subcontractors, including but not limited to the duty to cooperate, indemnify or provide insurance for the benefit of the covered entity. To maximize its protection, the covered entity may want to confirm in the BAA that the business associate is responsible for any acts or omissions of its subcontractors even if the subcontractors are independent contractors.

3.3.2.6 Termination and remedies. In addition to termination provisions required by HIPAA, the covered entity should ensure that a violation of the BAA allows the covered entity to terminate the underlying service agreement as well as the BAA. The covered entity may want to address additional remedies or processes related to such termination.

3.4 Do Not Work with Business Associates Who Will Not Comply. HIPAA imposes significant costs and obligations on business associates. Covered entities must respond to business associate violations. (45 CFR § 164.504(e)(1)). Beware business associates who are small, unsophisticated, or who simply do not understand or have the resources to comply with HIPAA, including individuals who perform services out of their homes or small offices. There is a good chance that such persons may be deemed to be agents of the covered entity. Even if they are not, the covered entity may eventually be required to address their HIPAA violations. At the very least, covered entities may need to ensure the business associate understands its obligations contained in HIPAA and the BAA. It is usually better to contract with entities that the covered entity knows will comply.

3.5 Do Not Disclose More PHI than Necessary. HIPAA's "minimum necessary rule" generally prohibits covered entities from using or disclosing more PHI than is necessary. (45 CFR § 164.502(b)). It is also a good risk management practice: business associates cannot improperly use or disclose PHI that they do not have. Where possible, covered entities should encrypt PHI and require business associates to do the same. Encryption is an addressable standard under the Security Rule. (45 CFR § 164.314(e)(2)(ii)). Encrypted data is considered secured for purposes of the Breach Notification Rule; accordingly, the loss of properly encrypted data need not be reported to the individual or HHS. (45 CFR § 164.402).

3.6 Do Not Impose Unreasonable or Unexpected Limitations. As a general rule, BAAs "may not authorize the business associate to use or further disclose the information in a manner that would violate the [HIPAA Privacy Rule] if done by the covered entity." (45 CFR § 164.502(e)(2)(i)). To the extent that the covered entity agrees to limit uses or disclosures through an agreement with the patient or by a notice of privacy practices that is more restrictive than HIPAA requires, those restrictions pass through to the business associate, *i.e.*, "each agreement in the business associate chain must be as stringent or more stringent as the agreement above with respect to the permissible uses and disclosures." (78 FR 5601) The problem is that such additional limitations or restrictions are not usually communicated to or anticipated by the business associate, resulting in unintentional violations. For that reason, the OCR's sample BAA provisions include terms that require covered entities to notify the business associate of such restrictions. (*See* https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html). Covered entities can protect themselves as well as their business associates by avoiding such agreements or limitations that are more restrictive than HIPAA requires.

3.7 Monitor Business Associates—or Not. Given the potential consequences of business associate misconduct, covered entities sometimes reserve the right to audit the business associate's policies or practices, assume the duty to confirm a business associate's compliance, and/or monitor the business associate's ongoing conduct. Although perhaps well-intentioned, covered entities are not required to actively monitor their business associates and doing so may actually increase the covered entity's potential liability as well as its cost of doing business.

As explained above, the Privacy and Security Rules only require that (1) the covered entity enter BAAs with business associates requiring them to comply with certain portions of HIPAA, and (2) if the covered entity learns that the business associate is noncompliant, then the covered entity must take reasonable steps to cure the violation or terminate the agreement. (*See* 45 CFR §§ 164.314, 164.504(e), and 164.504(e)(ii)). The rules do not require the covered entity to take affirmative steps to confirm the business associate's compliance or monitor the business associate's conduct. When the HIPAA Privacy Rule was first proposed, HHS suggested language that would require covered entities to take reasonable steps to ensure the business associate's compliance; however, it

abandoned that approach in the final rule because of the burden it would impose on covered entities. The relevant HHS commentary states:

> In the final rule, we reduce the extent to which a covered entity must monitor the actions of its business associate and we make it easier for covered entities to identify the circumstances that will require them to take actions to correct a business associate's material violation of the contract, in the following ways. We delete the proposed language requiring covered entities to "take reasonable steps to ensure" that each business associate complies with the rule's requirements. Additionally, we now require covered entities to take reasonable steps to cure a breach or terminate the contract for business associate behaviors only if they know of a material violation by a business associate. In implementing this standard, we will view a covered entity that has substantial and credible evidence of a violation as knowing of such violation. While this standard relieves the covered entity of the need to actively monitor its business associates, a covered entity nonetheless is expected to investigate when they receive complaints or other information that contain substantial and credible evidence of violations by a business associate, and it must act upon any knowledge of such violation that it possesses.

(65 FR 82505; *see also id.* at 82641). HHS further explained:

> We also believe it would be unnecessarily burdensome to require covered entities to monitor business associates' establishment of specific training requirements. Covered entities' responsibility for breaches of privacy by their business associates is described in §§ 164.504(e) and 164.530(f). If a covered entity believes that including a training requirement in one or more of its business associate contracts is an appropriate means of protecting the health information provided to the business associate, it is free to do so.

(*Id.* at 82745).

> The final rule reduces the extent to which an entity must monitor the actions of its business associates. The entity no longer has to "ensure" that each business associate complies with the rule's requirements. Entities will be required to cure a breach or terminate a contract for business associate actions only if they knew about a contract violation.

(*Id.* at 82785). HHS reaffirmed its position in its commentary to the final version of the Privacy Rule:

> The Privacy Rule does not require a covered entity to actively monitor the actions of its business associates nor is the covered entity responsible or liable for the actions of its business associates. Rather, the Rule only requires that, where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligations under the contract, the covered entity take steps to cure the breach or end the violation. See § 164.504(e)(1).

(67 FR 53252). More recently, the OCR published the following FAQ confirming the issue:

> **Is a covered entity liable for, or required to monitor, the actions of its business associates?**
>
> **Answer:** No. The HIPAA Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. Nor is the covered entity responsible or liable for the actions of its business associates. However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights. See 45 CFR § 164.504(e)(1)…. (Date Created: 12/19/2002)

(OCR FAQ available at https://www.hhs.gov/hipaa/for-professionals/faq/236/covered-entity-liable-for-action/index.html).

A covered entity may choose to affirmatively monitor or confirm its business associate's compliance, but it should carefully consider the pros and cons of doing so. Obviously, confirming the business associate's compliance helps protect against a breach that may adversely affect the covered entity as well as the business associate, and may demonstrate the covered entity's reasonable actions if claims are brought against it. On the other hand, implementing such reviews may be very costly and burdensome. In addition, it might actually increase the potential liability of covered entities. A covered entity may create an agency relationship if it exerts too much control over the business associate, thereby making the covered entity vicariously liable for the business associate's violations. (*See* 45 CFR § 160.402(c); 78 FR 5581). Also, by taking on itself the duty to review the policies and practices of its business associate, a covered entity may assume the duty to perform the review in a competent manner and may be liable for failing to do so. At the very least, the review may uncover violations that would trigger the covered entity's obligations to respond with associated cost and exposure—obligations and exposure that the covered entity would not have if it did not know of the violation. To some extent, ignorance is bliss when it comes to HIPAA violations. For these reasons, a covered entity may conclude it is better off not assuming such optional duties or looking for trouble.

3.8 Respond Promptly to Violations. Although covered entities are not required to actively monitor business associates, they must promptly respond and document their actions if they have substantial and credible knowledge of a violation. (65 FR 82505). Prompt action is important for several reasons:

First, covered entities have an affirmative obligation to cure business associate violations and mitigate improper disclosures. (45 CFR §§ 164.501(e)(1) and 164.530(f)). While they may not be liable for the business associate's misconduct, covered entities are liable for their own failure to act when required. In fact, the failure to respond may constitute willful neglect on the part of the covered entity, exposing it to mandatory penalties. (*See* 75 FR 40879).

Second, covered entities may avoid HIPAA penalties if they do not act with willful neglect and correct a violation within thirty (30) days. (45 CFR § 160.410(b)). Although it may not be able to "unring" the bell, a covered entity may ensure that the bell does not continue ringing by, *e.g.*, changing processes; implementing new safeguards; modifying policies; training employees; and/or terminating BAAs. (*See* 75 FR 40879).

Third, covered entities have an affirmative obligation to report breaches of unsecured PHI unless they can demonstrate a low probability that the data has been compromised. (45 CFR § 164.400 *et seq.*). Timely mitigation is one of the four factors used to evaluate whether the data has been compromised. (45 CFR § 164.402).

To ensure timely action, "[c]overed entities should ensure their [business associates,] workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so." (74 FR 42749). Including appropriate terms in the BAA may help ensure timely reports.

If the business associate's conduct has resulted in a potentially reportable breach of unsecured PHI, the covered entity should err on the side of reporting the breach. In most cases, the covered entity will not be liable for the business associate's breach; however, failure to timely report the breach may constitute "willful neglect", subjecting the covered entity to mandatory penalties for its own inaction. HHS gave the HHS gave the following example of conduct constituting "willful neglect":

> A covered entity's employee lost an unencrypted laptop that contained unsecured protected health information. HHS's investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 et seq.

(75 FR 40879). Accordingly, it is usually safer for the covered entity to report the breach and lay blame on the business associate instead of trying to cover up or ignore the breach.

3.9 Terminate the BAA if Necessary. The BAA must "authorize termination of the contract by the [CE], if the [CE] determines that the [BA] has violated a material term of the contract." (45 CFR § 164.504(e)(2)(iii)). Covered entities must terminate the BAA if violations cannot be cured. (45 CFR § 164.504(e)(1)). Covered entities should ensure that the underlying services agreement coordinates with the BAA termination provisions; however, even if they do not, HIPAA would preempt contrary contract provisions and allow termination.

3.10 Ensure the PHI is Retrieved, Destroyed or Protected. Upon termination of the BAA, the business associate must,

> if feasible, return or destroy all [PHI] received from, or created or received by the [BA] on behalf of, the [CE] that the [BA] still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(45 CFR § 164.504(e)(2)(ii)(J)). It may be helpful to obtain certification from the business associate that it and its subcontractors have complied with these provisions. These provisions would preempt any contrary terms in the service agreement and prohibit the business associate's attempt to retain or use PHI improperly, including to hold the PHI hostage in a payment dispute. The OCR published the following FAQ, which may be helpful in addressing such situations:

> **May a business associate of a HIPAA covered entity block or terminate access by the covered entity to the protected health information (PHI) maintained by the business associate for or on behalf of the covered entity?**

> **Answer:** No…. [A] business associate may not use PHI in a manner or to accomplish a purpose or result that would violate the HIPAA Privacy Rule. See 45 CFR § 164.502(a)(3). Generally, if a business associate blocks access to the PHI it maintains on behalf of a covered entity, including terminating access privileges of the covered entity, the business associate has engaged in an act that is an impermissible use under the Privacy Rule. For example, a business associate blocking access by a covered entity to PHI (such as where an Electronic Health Record (EHR) developer activates a "kill switch" embedded in its software that renders the data inaccessible to its provider client) to resolve a payment dispute with the covered entity is an impermissible use of PHI. Similarly, in the event of termination of the agreement by either party, a business associate must return PHI as provided for by the business associate agreement. If a business associate fails to do so, it has impermissibly used PHI….
>
> [The] OCR notes that a covered entity is responsible for ensuring the availability of its own PHI. To the extent that a covered entity has agreed to terms in a business associate agreement that prevent the covered entity from ensuring the availability of its own PHI, whether in paper or electronic form, the covered entity is not in compliance with 45 CFR §§ 164.308(b)(3), 164.502(e)(2), and 164.504(e)(1).

(OCR FAQ dated 9/23/16, available at https://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html).

4. CONCLUSION

The OCR has many means to hold covered entities liable for the misconduct of their business associates. To avoid such situations, the best defense is a good offense: covered entities should ensure that they comply with their own HIPAA obligations, including identifying and executing appropriate BAAs. Although it is tempting to attempt to control business associates, covered entities should refrain from doing so unless they are willing to exercise such control appropriately and accept liability for the business associate's misconduct. In most cases, cost and potential liability will be reduced by treating the business associate as an independent contractor and documenting same. If there are violations or concerns, the covered entity should take prompt action to respond. By doing so, it should be able to avoid HIPAA penalties for the business associate's misconduct.

For questions regarding this update, please contact: Kim C. Stanger at kcstanger@hollandhart.com or 208-383-3913.