manatt

Business Associate Compliance With HIPAA: Findings From a Survey of Covered Entities and Business Associates

Deven McGraw, Partner, Healthcare Industry, Manatt, Phelps & Phillips, LLP

Susan Ingargiola, Director, Manatt Health Solutions

Kier Wallis, Manager, Manatt Health Solutions

Note: This paper was funded by The California HealthCare Foundation.

I. Introduction

The delivery of health care – and payment for that care – is a complex endeavor, and health care providers and health plans rely on third parties to help them operate as businesses and fulfill their responsibilities to patients and beneficiaries. Frequently, these third parties need access to health information in order to perform functions or services for health care entities. The Health Insurance Portability and Accountability Act or "HIPAA"[1] permits health care providers and health plans (known as "Covered Entities") to share health information with these third party vendors, which are referred to as "Business Associates" under HIPAA's regulations. Historically, HIPAA regulated Business Associates by requiring Covered Entities to manage them through contractual relationships. However, in 2009, Congress made Business Associates directly accountable to regulators for compliance with most of HIPAA's regulations, and regulations to effect that change were finalized in 2013. With this enhanced accountability come questions about the extent to which Business Associates are in compliance with HIPAA's privacy and security rules.

In an effort to assess Business Associates' compliance with their obligations to protect health information under HIPAA, this report provides an overview of the different types of services that Business Associates provide to Covered Entities, describes the efforts that Business Associates and Covered Entities are making to satisfy HIPAA's various privacy and security requirements, and makes recommendations to improve these efforts. The report was informed by telephone interviews with 16 Covered Entities (representing large health systems, integrated delivery networks, small physician offices, health centers, pharmacies, health plans and government payers) and five Business Associates (representing technology and software vendors and health information networks).[2]

The interviews were structured to answer the following questions, among others:

- What types of organizations are Business Associates?
- What common issues arise for Covered Entities with respect to management of their Business Associates?
- What common issues arise for Business Associates with respect to complying with HIPAA?
- What are the best ways to reach and educate the Business Associate community to assure its compliance with HIPAA on an ongoing basis?

This report begins by defining and describing the legal framework governing Business Associates. It then summarizes Covered Entities' answers to questions on the following topics:

- Number and size of contracted Business Associates;
- Types of services performed by Business Associates;
- Sophistication levels of Business Associates;
- Efforts to evaluate Business Associates' capacity for compliance (i.e., "due diligence efforts");
- Interactions with Business Associate personnel and experience negotiating Business Associate Agreements ("BAAs");
- Ongoing oversight of Business Associate compliance;
- Experience working with Business Associates during a breach;
- Rules governing Business Associates' handling and return or destruction of protected health information; and
- Perception of Business Associate compliance after enactment of the Health Information Technology for Economic and Clinical Health ("HITECH") Act.[3]

Next, the report summarizes Business Associates' answers to questions about their ability to comply with HIPAA and, specifically, their efforts to train their workforce on HIPAA compliance. The report concludes by recommending several strategies for improving Business Associate compliance with HIPAA, particularly those doing business in California.

II. Legal Landscape Governing Business Associates

a. HIPAA

HIPAA is the principal federal law regulating health information privacy. It applies to "Covered Entities," which broadly consist of health care providers, health insurers, and health care clearinghouses (entities that convert data from HIPAA standard formats to non–standard formats – or vice versa – in connection with certain types of transactions carried out between providers and health plans).[4] The HIPAA Privacy Rule — the regulations implementing HIPAA's privacy protections — establishes the circumstances under which "protected health information" ("PHI") (information that does or can identify an individual) can be accessed, used, or disclosed, and grants individuals certain rights to their own health information.[5] The HIPAA Security Rule mandates appropriate safeguards — administrative, physical, and technical — to help ensure the confidentiality, integrity, and security of PHI stored electronically.[6]

i. Definition of a Business Associate

In addition to Covered Entities, HIPAA also addresses "Business Associates" that, on behalf of a HIPAA Covered Entity, perform functions or services that include PHI.[7] An entity qualifies as a Business Associate if it "creates, receives, maintains, or transmits" PHI "on behalf of" either a Covered Entity or a Business Associate (e.g., if it is a subcontractor of a

Business Associate).[8] Not all outside vendors or service providers that have relationships with a Covered Entity qualify as Business Associates under HIPAA. Specifically, a Business Associate is a person or entity who is not a member of the Covered Entity's workforce and is performing a function or activity involving the use or disclosure of PHI.

According to guidance from the Office for Civil Rights ("OCR") within the U.S. Department of Health and Human Services ("HHS"), which is responsible for overseeing and enforcing HIPAA, the following are examples of services that could give rise to a Business Associate relationship if they are performed on behalf of a Covered Entity and involve PHI: billing, language translation/interpretation, transcription, peer review, quality assurance, utilization review, practice management, claims processing or administration, claims repricing, data analysis, temporary staffing services, software development/maintenance, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services.[9] Additional examples include third party administrators, pharmacy benefit managers to a health plan, and patient safety organizations under the Patient Safety and Quality Improvement Act.[10] Entities such as regional health information organizations and health information exchanges ("HIEs") that facilitate the exchange and sharing of information among providers also meet the definition of a Business Associate.[11]

ii. Direct Regulation of Business Associates Under HIPAA

Historically, HIPAA did not directly apply to Business Associates and their subcontractors. Instead, Covered Entities were required to obtain satisfactory written assurances (in the form of a "Business Associate Agreement" or "BAA") that their Business Associates would: (1) use PHI only for the purposes for which they were engaged by Covered Entities; (2) safeguard PHI from misuse; and (3) cooperate with and help Covered Entities comply with their responsibilities under the Privacy Rule.[12]

In 2009, Congress changed this in the HITECH Act. Business Associates now are subject to civil and, in some cases, criminal penalties for making uses and disclosures of PHI in violation of HIPAA or their BAAs.[13] Business Associates are also directly liable and subject to civil penalties for failing to safeguard electronic PHI in accordance with the HIPAA Security Rule.[14] Importantly, HITECH grants HIPAA enforcement authority to state attorneys general, meaning that state authorities may pursue remedies for a HIPAA violation if HHS or another federal department does not.[15] Generally, there is no private right of action under HIPAA (i.e., individuals cannot sue Covered Entities or Business Associates for violations of HIPAA).

b. State Privacy Laws and Legal Action

Many states have enacted statutes that protect the privacy and security of health information.[16] HIPAA preempts (or invalidates) state laws that conflict with it or provide less protection for privacy but state laws that are more protective continue to apply.[17] In California, a HIPAA Business Associate also is likely covered under the state's Confidentiality of Medical Information Act (the "CMIA").[18] Under the CMIA, the state attorney general, a county counsel, district attorney, or city attorney may bring a civil action to enforce the CMIA, and individuals may sue for damages arising from any negligent release of confidential information.[19]

In addition, individuals can sue Covered Entities and Business Associates (and others) for violations under the common law principles of invasion of privacy, defamation, negligence and breach of fiduciary duty, among others. Business Associates may also be sued by their Covered Entities for breaching the terms of their BAAs.

III. Summary of Covered Entity Interviews

a. Number, Size and Organizational Characteristics of Business Associates Used by Covered Entities

Key Themes

- Keeping an accurate count of Business Associates is a challenge for large Covered Entities, due to volume and that origination and management of Business Associate relationships frequently occurs throughout the organization.
- The number and size of Business Associates used by Covered Entities varies widely.

The number of Business Associates reported or estimated by the Covered Entities interviewed for this report varied widely and ranged from as low as four to as high as 10,000. Generally, smaller Covered Entities, such as independent physician practices and health centers, contract with only a handful of Business Associates while larger Covered Entities, such as health plans and health systems operating in multiple regions across the country, contract with thousands. Most of the larger Covered Entities were only able to estimate the number of their Business Associates. Often there are multiple points of origination for Business Associate relationships throughout their organizations (i.e., Business Associates can be hired and managed by various "business units" and may not be managed by the legal or compliance office), making it difficult to catalogue all Business Associates in one place or have confidence in an absolute number. While some of the larger Covered Entities

reported using an electronic database to track their Business Associates, they noted the possibility, for the reason stated above and others, that a significant number of Business Associates may not be included in the database. In some cases, the primary function of this database is to track vendor relationships, some of which may not be Business Associates. Many Covered Entities reported that their Compliance Departments considered purchasing software that would enable them to keep better track of their Business Associates but ultimately their institutions or organizations decided to allocate resources to higher priorities.

There also is a wide range in the size of the Business Associates with which Covered Entities contract, ranging from small, "mom and pop" businesses to large organizations with national or even international operations.

"In a big health system like ours, our Business Associate population is enormous thanks to the high volume of contracts we have across the system and at each individual facility. The BAA template is out there for business units to use, and the lawyers don't always see or even know of the agreement."

b. Types of Services Performed by Business Associates, Determining Which Vendors Are Business Associates

Key Themes

- Business Associates perform a wide array of services for Covered Entities.
- Covered Entities frequently characterize all vendors as Business Associates in order to be conservative with respect to legal compliance and to have a more efficient one–size–fits–all approach to managing vendors.

The types of services performed by Business Associates for Covered Entities vary widely. Covered Entities reported contracting with Business Associates for the following types of services, among others:

- Transcription services
- Accreditation
- Registry management
- Data center hosting
- Care management
- Utilization monitoring
- Provider credentialing
- Quality improvement
- Research
- Electronic health records and health information exchange services
- Practice management and billing services
- Claims coding
- Customer service
- Various IT support functions
- Software application development
- Malpractice insurance
- Payment lock box services

Many Covered Entities take a self–described "conservative approach" and treat all or nearly all entities with whom they have business relationships as Business Associates. This allows them to deploy one–size–fits–all organization–wide policies and agreements; avoids spending resources determining or negotiating over whether a business partner is or is not a Business Associate, and feels "better safe than sorry" from a regulatory compliance standpoint. For example, several Covered Entities require other health care providers, who are also Covered Entities and who are receiving PHI for their own treatment or health care operations purposes, to sign BAAs. At least one Covered Entity specifically requires its landscapers to sign BAAs because they could conceivably come into contact with PHI during the course of their work. There are challenges associated with this approach, however. For example, under a standard BAA, a Business Associate is meant to serve as a temporary custodian of the Covered Entity's PHI and is obligated to use the PHI only to serve the Covered Entity (and to return or destroy the PHI when the BAA terminates). This framework does not apply when a health care provider receives PHI from another health care provider for its own treatment purposes. That is, the receiving provider will likely incorporate the PHI it receives into its own records and will maintain it indefinitely rather than return or destroy it. Further, the receiving provider will not be using the PHI to serve the disclosing provider but will instead be using it for its own purposes. In these types of situations, there could actually be a conflict between the terms of the BAA and the manner in which the parties operate in practice.

Another Covered Entity interviewed for the report anticipates that that the scope of its relationship with a vendor may change over time. Even in circumstances where the vendor does not initially have access to PHI, this entity's standard vendor agreement includes a provision obligating the vendor to comply with its BAA provisions to the extent the vendor has access to PHI. The entity believes this approach negates the need to re–evaluate the BA status of the vendor every time the scope of work changes. In contrast, other Covered Entities define "Business Associate" narrowly and prefer to take the time "up front" to determine whether a vendor is by law a Business Associate in order to avoid time on the "back end" negotiating a BAA and attending to all of the obligations associated with the Business Associate relationship if such activities are not truly necessary.

Legally HIPAA does not require the type of conservative approach to identifying BAs that is described above, and the treatment of an entity as a Business Associate by a Covered Entity does not translate into Business Associate liability under the law. For example, persons or organizations whose functions, activities, or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, are not Business Associates.[20] Further, any member of the Covered Entity's workforce, which includes employees, volunteers, trainees, and other persons under the direct control of a Covered Entity, whether paid or unpaid, is not a Business Associate.[21] The term "Business Associate" also does not include a health care provider with respect to disclosures by a Covered Entity to the health care provider concerning the treatment of an individual (e.g., a primary care physician disclosing PHI to a contract specialist or a physician disclosing PHI to a pharmacy to provide a prescription drug to an individual). Several Covered Entities reported confusion among banks and other financial institutions about whether they met the definition of a Business Associate. HHS OCR has released guidance that, under HIPAA, a bank or other financial institution that does no more than process consumer–conducted financial transactions by debit, credit or other payment card, clear checks, initiate or process electronic funds transfers, or conduct any other activity that directly facilitates or effects the transfer of funds, is not a Business Associate.[22]

"We like to be conservative and have contractors sign BAAs if there is any chance they may encounter PHI."

c. Business Associates and Sophistication About HIPAA

Key Themes

- Most Business Associates, especially larger ones, have individual roles or offices dedicated to HIPAA compliance; for Covered Entities, the absence of a designated role or office is a clue to a Business Associate's lack of sophistication about HIPAA.
- Smaller Business Associates that are new to the health care industry (e.g., software vendors) are more likely to be unfamiliar with their obligations under HIPAA.

Some Covered Entities reported that the majority of their Business Associates were "sophisticated" (i.e., were aware that they fell within the definition of a Business Associate and had processes in place to comply with HIPAA and their BAAs) and that the level of Business Associate sophistication has improved over the last 10 years.

Other Covered Entities reported a range of sophistication among their Business Associates. Generally, smaller Business Associates and Business Associates that are not themselves part of the health care sector (e.g., financial institutions and non–health related software companies) are less likely to be aware of HIPAA and its requirements. When Business Associates are smaller, new to health care and/or unfamiliar with their obligations under HIPAA, it places significant stress on the business relationship between the two entities, and Covered Entities have greater concerns about the Business Associates' ability and intent to comply.

One Covered Entity reported that having to negotiate a BAA with a Business Associate's lawyer who is not familiar with HIPAA can be an extremely arduous process. Another Covered Entity voiced concern that few smaller Business Associates take their HIPAA compliance obligations seriously and most "aren't doing anything." On the topic of software vendors, this Covered Entity noted that "PHI is just data to information technology ("IT") vendors; they aren't necessarily thinking about compliance or how their obligations are different because the data is PHI."

Of the more "sophisticated" Business Associates (i.e., those that are familiar with their obligations under HIPAA), many have a specific person who is responsible for the organization's compliance. Often, this person is the "Compliance Officer" or "Privacy Officer." Larger organizations tend to have an entire team or department dedicated to compliance and privacy. The absence of any particular person or office at the Business Associate responsible for privacy law compliance is, for many Covered Entities, an early (and often alarming) indication of a lack of sophistication about HIPAA.

d. Covered Entities' Efforts to Evaluate Business Associates' Capacity for Compliance (i.e., "Due Diligence")

Key Themes

- Covered Entities do not feel they have enough resources to thoroughly evaluate Business Associates' compliance with HIPAA and the terms of their BAAs.
- In light of their limited resources, most Covered Entities only perform investigations of "high risk" Business Associates' capacity for compliance (e.g., those Business Associates that access electronic PHI).
- Covered Entities rely on their IT staff's expertise when evaluating a Business Associate's security policies and practices.

Covered Entities generally feel as though they do not have enough resources to thoroughly evaluate a prospective Business Associate's ability to comply with HIPAA and the

terms of its BAA. Most of the Covered Entities interviewed performed little to no due diligence on prospective Business Associates – with the exception of Business Associates providing IT services that have access to electronic PHI. Covered Entities (particularly larger Covered Entities) generally consider these contracts high risk enough to warrant the devotion of resources to investigation of the Business Associate's security policies and processes before signing a BAA. These investigations are often performed by Covered Entities' IT staff, on whom the Covered Entities' compliance departments rely for expertise.

When diligence is performed (most often by larger Covered Entities), the key tool in the process is generally a questionnaire that the business units transmit to the Business Associate, which queries the Business Associate on various aspects of HIPAA compliance (e.g., disclosure policies, security tools, training, etc.). The Covered Entities generally use the answers to stratify the vendor into a risk category, dictating the level of additional investigation required before the Covered Entity will sign the BAA, as well as the need for continued oversight post–BAA. For example, one Covered Entity reported calling in subject matter experts to work with a vendor to ensure its security protocols met the Covered Entity's requirements. Once the Covered Entity's legal /compliance team was satisfied that the Business Associate could meet the Covered Entity's requirements, the business unit was permitted to sign the BAA.

Even in circumstances where Covered Entities feel due diligence of Business Associates is necessary, they noted difficulties in balancing diligence needs with the business need to execute contracts in a timely manner. Some Covered Entities have developed a work–around, allowing time sensitive contracts to be executed right away, with due diligence performed later, with provisions in the BAA to allow the Covered Entity to revisit the contract if the due diligence surfaces a concern.

One Covered Entity noted that when a Business Associate resists a Covered Entity's requests for information on which to assess the Business Associate's ability to comply with HIPAA, it should be considered a red flag for future issues regarding HIPAA compliance.

"The level of due diligence we use depends on the Business Associate's service, size and sophistication. If the Business Associate is a large hospital, health plan or pharmaceutical company, due diligence is easy. It is also relatively easy if the Business Associate is a small physician practice that has very little by way of HIPAA compliance practices. It is harder to evaluate organizations that fall in the middle ground. The business imperative to contract often overrides HIPAA compliance."

e. Covered Entities' Interactions With Business Associate Personnel and Experiences Negotiating BAAs

Key Themes

- Larger Business Associates have Compliance Departments; when a Business Associate does not have a Compliance Department, it generally relies on its business managers to coordinate with a Covered Entity on HIPAA compliance matters.
- Covered Entities prefer to use their standard BAA template, which often tracks the BAA template created by HHS OCR.
- When negotiations of a BAA occur between a Covered Entity and a Business Associate, they often relate to provisions that are not mandated under HIPAA (e.g., indemnification and breach notification time frame provisions).

As a general matter, larger Business Associates have compliance or legal departments, and a representative from one of those departments typically serves as the main point of contact for the Covered Entity both during the negotiation of the BAA and throughout the business relationship with the Covered Entity. However, some Covered Entities reported that a business person serves as their main point of contact within a Business Associate.

With respect to BAAs, many Covered Entities "use their own paper" – i.e., they ask Business Associates to execute the Covered Entity's standard version of a BAA, which generally tracks the model BAA issued by OCR but often includes "additional" provisions that are not required under HIPAA. Business Associates are then expected to review and sign the BAA. Most Covered Entities receive little "push back" on the standard, required provisions of their BAAs . However, many Covered Entities reported having Business Associates attempt to negotiate the "additional" provisions, which often relate to liability for mishandling of PHI or other violations and indemnification of the Covered Entity by the Business Associate for the costs associated with such violations. For example, Covered Entities sometimes include provisions that would require their Business Associates to indemnify them for the costs they would incur to notify individuals of a breach of their PHI by the Business Associate.

Specifically, Covered Entities reported relatively frequent negotiations with Business Associates over BAA provisions relating to breaches, including the time frame in which the Business Associate is required to report a suspected or actual

breach to the Covered Entity, who (the Covered Entity or the Business Associate) is responsible for determining whether a breach actually occurred, who is responsible for notifying individuals of a breach of PHI, and, as referenced above, who is responsible for the costs associated with a breach.

In the view of some Covered Entities, whether a Business Associate attempts to negotiate the provisions of a BAA that are not statutorily mandated under HIPAA can reflect the level of sophistication of the Business Associate. In other words, if the Business Associate attempts to negotiate these provisions in a BAA, then the Business Associate is probably "paying attention" to its obligations to safeguard the Covered Entity's PHI by complying with HIPAA and the terms of the BAA.

f. Covered Entities' Ongoing Oversight of Business Associate Compliance

Key Themes

- Covered Entities employ varying levels of oversight over Business Associates' compliance with HIPAA and their BAAs.
- Most Covered Entities do not audit their Business Associates' compliance; those that do tend to focus on their Business Associates' compliance with HIPAA's security requirements.
- Most Covered Entities do not ask to see their Business Associate's HIPAA–required risk analysis or policies and procedures.

Historically, covered entities historically could not be held liable for their Business Associates' HIPAA violations if the Covered Entity had an appropriate BAA in place and either did not know of the Business Associate's breach of the agreement or took reasonable steps to cure the breach and terminated the agreement or reported the problem to HHS if such steps were unsuccessful.[23] As noted above, HITECH made Business Associates directly accountable to regulators for failure to comply with the HIPAA Security Rule and certain provisions of the HIPAA Privacy Rule. Notwithstanding that HIPAA has never made Covered Entities liable for the improper actions of independent Business Associates, many Covered Entities have historically felt more comfortable having some oversight of their Business Associates, and this pattern persists even post–HITECH.

For Covered Entities, managing Business Associates (i.e., identifying which contractors are properly identified as Business Associates, performing due diligence, entering into a BAA, monitoring the Business Associates' ongoing compliance with the terms of the BAA, and ensuring the return or destruction of PHI at the end of relationship, among other things) is a highly resource–intensive endeavor. In cases where a Covered Entity's Business Associates number in the thousands or even tens of thousands, it is practically impossible. Consequently, it is not surprising that Covered Entities reported varying levels of ongoing oversight of Business Associates' compliance with HIPAA and their BAAs.

When asked about their efforts to monitor the compliance of their Business Associates with HIPAA or their BAA, several Covered Entities reported that when they weigh the cost of performing oversight with the risks of a breach or other violation by a Business Associate, the costs outweigh the potential benefits of ongoing monitoring. According to one Covered, Entity, "there is a law of diminishing returns when it comes to auditing Business Associates." However, some large Covered Entities perform audits of certain "high risk" Business Associates. For example, one health plan's IT/security staff conducts routine audits of vendors that handle electronic PHI, while its global business service team audits and oversees the security practices of offshore vendors. The health plan is piloting a privacy–focused audit with two of its larger vendors that it considers to be higher risk. The audit begins with an "external service provider questionnaire" and is followed by an onsite walk through with the vendor's privacy and security team. If successful, the health plan intends to make this assessment part of its standing annual privacy review process. Another Covered Entity reported that it regularly audits the practices of its Business Associates and that the costs of these audits are paid for by the business units that use the Business Associates' services.

Generally, smaller Covered Entities do not have the resources to engage in any type of ongoing monitoring of the privacy and security activities of their Business Associates. Some Covered Entities contractually mandate that their Business Associates have written privacy and security policies and procedures, but they do not request to see them. None of the Covered Entities interviewed have asked to review a Business Associate's HIPAA–mandated security risk analysis before entering into a BAA. Several Covered Entities hypothesized that most Business Associates have not performed risk analyses despite the legal mandate that they do so. On the other hand, several Covered Entities noted that their BAAs require Business Associates to attest (or represent and warrant) that they have performed the risk analysis and have adopted the necessary policies and procedures, which acknowledge the Business Associate's responsibility but without Covered Entity review.

> "HIPAA is an overwhelming topic; you can't just buy [HIPAA compliance] off the shelf."

g. Covered Entity's Experiences with Business Associates During a Breach

Key Themes

- Differences in legal obligations on Covered Entities under federal and state law make compliance with breach notification requirements challenging for Covered Entities and Business Associates alike.
- Covered Entities interviewed for this paper have not received many breach reports from Business Associates.

HITECH requires HIPAA–Covered Entities to notify individuals in the event of a "breach," which is defined as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information.[24] In the event of a breach, Business Associates of a Covered Entity must notify the Covered Entity, which in turn must notify the individual within 60 days after the breach is discovered.[25]

California also has state statutes addressing health information breaches.[26] Organizations covered under the CMIA (e.g., clinics, health facilities, home health agencies and hospices) must notify affected individuals of a breach, as well as notify the California Department of Public Health.[27] They have only five business days after discovering a breach of medical information to report it, and only law enforcement may request a delay in such notice.[28] Further, any person or business that conducts business in California must notify individuals when there has been a breach involving health information that is not secured through encryption if the information is "reasonably believed to have been acquired by an unauthorized person."[29]

California's breach laws differ from federal law in important ways, including but not limited to the timeframe within which breach notifications must be made. Managing these differences can be challenging for Covered Entities and Business Associates alike. Several Covered Entities not subject to California law (or any state law with short breach notification reporting timelines) require their Business Associates to notify them of a security incident or potential breach or other security incident within 10 days post–discovery. This time period gives Covered Entities enough time to comply with HIPAA's 60 day deadline, and enables them to work with the Business Associate to determine whether or not the breach triggers a reporting obligation. Covered Entities subject to California's 5–day notification timeline, on the other hand, generally require Business Associates to notify them of suspected breaches or security incidents immediately. Business Associates outside of the health care sector are frequently surprised by the heightened requirements of California law.

One Covered Entity reported as a significant breach–related challenge the ability to locate the right contact person within the Business Associate in the event of a breach. This Covered Entity reported that during one breach situation, it took 24 hours to identify someone within the Business Associate who had the authority to address the issue. This can be particularly challenging when Covered Entities do not have processes in place to ensure Business Associates' contact information remains accurate or to confirm whether the individual who signed the BAA had/has authority to bind the organization. When a Covered Entity has thousands of Business Associates, and where BAAs are often negotiated and managed by business units, keeping track of this information is no minor task.

The Covered Entities interviewed reported receiving relatively few notifications of breaches by their Business Associates. Of those relatively few breaches, most were not IT–security violations by outside hackers. Rather, most reported breaches were the result of some type of human error (e.g., an individual stuffing one person's test results into another person's envelope). Nevertheless, Covered Entities generally expressed concern that there is no way to reliably determine whether a Business Associate has failed to notify the Covered Entity of a breach as required, since Covered Entities are not privy to the day–to–day operations of their Business Associates. At least one Covered Entity said that a lack of reporting of security incidents is more likely to indicate a Business Associate's lack of awareness of its obligation to report than a lack of security incidents.

> "We would prefer to be notified of any potential security incidents or unauthorized disclosures and work collaboratively with our Business Associates to resolve the matter and make notifications as appropriate."

h. Rules Governing Business Associates' Handling and Return or Destruction of PHI

i. Storing PHI Offshore

Key Themes

- Most Covered Entities do not permit their Business Associates to store PHI offshore.
- When they do so, the Covered Entity may engage in a more thorough review of the Business Associate's security systems.

The HIPAA Privacy and Security Rules do not dictate where paper or electronic PHI may or may not be maintained, so Covered Entities and Business Associates are not prohibited from storing PHI outside of the United States (though there are

other laws that may restrict the practice of storing PHI offshore; for example, some state Medicaid programs prohibit the offshoring of Medicaid data). Therefore, whether to store PHI offshore is often a business decision made by the Business Associate. However, if there is a data breach involving an offshore vendor, the ability of OCR or even a state attorney general to take enforcement action against the offshore vendor is less certain. The foreign Business Associate could be subject to a breach of contract claim for violation of the BAA, but HIPAA, unlike certain other federal statutes, does not have explicit extra–territorial reach to enable federal or state regulators to bring an enforcement action. Further, HHS may have limited resources to pursue a foreign Business Associate.

In light of this, many Covered Entities do not allow their Business Associates to store their PHI in other countries. However, some do permit it. A number of Covered Entities who allow offshore storage of PHI engage in a higher degree of due diligence before signing a BAA. For example, one Covered Entity sends staff to visit the foreign Business Associate's facilities and requires that the Business Associate have strict policies and procedures in place to secure the data (i.e., employees are not allowed to bring phones with cameras into the workplace where PHI may be exposed). Other Covered Entities subject Business Associates that store their data offshore to more stringent and frequent audits. Still another Covered Entity requires executive–level approval from within the Covered Entity's organization before it agrees to allow a Business Associate to store PHI offshore; it also limits the countries in which PHI may be stored (e.g., it prohibits the storage of data in Iraq).

ii. Use of De–Identified Data for Commercial Purposes

Key Themes

- Most Covered Entities do not permit their Business Associates to de–identify their PHI and use it for commercial purposes even though it is permitted under HIPAA.
- Some Covered Entities have not had to set policies on this issue because no Business Associates have asked for this authority.

There are no restrictions on the use or disclosure of de–identified health information under the HIPAA Privacy or Security Rules, and HIPAA allows Business Associates to de–identify data if such authority is granted in the BAA.[30] De–identified health information neither identifies nor provides a reasonable basis to identify an individual.[31] Most Covered Entities do not allow Business Associates to use de–identified data for commercial purposes even though HIPAA permits it. However, some Covered Entities reported that use of de–identified data by Business Associates has not been an area of focus; no Business Associates have requested permission to de–identify data so they have not yet had to evaluate the issue. One Covered Entity with experience in evaluating Business Associate requests to de–identify data conditions this authorization on granting the Covered Entity access to any research done with de–identified data.

iii. Return or Destruction of PHI

Key Themes

- Most Covered Entities do not have processes in place to ensure that Business Associates destroy or return PHI when the relationship ends.
- Of those that do, the manager of the business relationship (and not the legal or compliance office) generally plays an important role in the process.

Under HIPAA, Business Associates must return to Covered Entities, or destroy, all PHI at the termination of the BAA so that the Business Associate maintains no copies of the information in any form. If such return or destruction is not feasible, the Business Associate must extend the protections of the BAA to the retained information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.[32]

Most Covered Entities reported that while their standard BAA requires that data be returned or destroyed, they do not have a process in place to ensure that the Business Associate has complied. For example, there is no process in place to notify compliance leadership when a contract has been terminated since it is typically the business relationship owner – not the legal/compliance department – that is engaged with the vendor at that point in the relationship.

However, some Covered Entities do have processes in place to address Business Associates' handling of data at the end of their contract. For example, one Covered Entity said that its legal/compliance department sends a return/destruction form to the business relationship owner once the purchasing department notifies the legal/compliance department that a contract is expiring. If the contract is not being renewed, the business relationship owner asks whether the Business Associate handled PHI and, if so, how it will ensure the return or destruction of the information. If applicable, the Covered Entity asks the Business Associate to sign an attestation that the PHI was destroyed. If destruction is infeasible, the Business Associate must notify the Covered Entity in writing and state that it will maintain the PHI in compliance with HIPAA.

Another Covered Entity generally does not allow Business Associates to store the Covered Entity's PHI locally in the

Business Associate's systems. When local storage is required for the Business Associate to perform its services, the Covered Entity requires the Business Associate to return or destroy the data immediately after the service has been performed (e.g. on the same day as opposed to at the end of the contract period).

"Our standard BAA does not allow for de–identification, but we get push back on occasion. Ultimately it's a business decision."

i. Covered Entities' Perceptions of Business Associate Compliance after HITECH

Key Themes

- Vendors of cloud storage services are now more likely to consider themselves to be Business Associates.
- Covered Entities' perceptions of Business Associate compliance with HIPAA after HITECH's enactment vary widely: some view Business Associate direct accountability to regulators as a positive development, while others believe it makes little difference.
- Some Covered Entities believe that direct regulation of Business Associates under HIPAA has made BAAs unnecessary.

As described above, HITECH expanded the definition of a Business Associate under HIPAA to include certain data transmission vendors and personal health record vendors, as well as health information organizations and electronic prescribing (e–prescribing) gateways. Notably, HHS distinguished between vendors that *transmit* PHI from vendors that *maintain* PHI on behalf of Covered Entities. The former are Business Associates only if they routinely access PHI; if not, they are ''conduits,'' such as internet service providers, that are outside the scope of HIPAA. In contrast, vendors that maintain PHI are Business Associates even if they do not require routine access to the PHI. This interpretation would appear to impose HIPAA requirements on certain cloud computing companies and other data storage vendors that previously took the position they were not Business Associates. To this end, the Covered Entities interviewed said that companies that previously argued they did not meet the definition of a Business Associate have now begun to sign BAAs.

HITECH also clarified that subcontractors of a Business Associate are Business Associates. Previously, a Business Associate was defined as an entity that performed certain functions for or on behalf of a *Covered Entity*, and subcontractors of Business Associates were presumed not to be covered. HITECH changed that framework by providing that a Business Associate also includes ''a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.''[33] As a result, subcontractors all the way down the contractual chain from Covered Entities have the same compliance obligations under HIPAA. A few Covered Entities reported that, as a result of this provision, they have begun probing more closely into the organizations with whom their Business Associates are sharing information and that they have placed more emphasis on ensuring that their Business Associates understand that they must enter into BAAs with their subcontractors. These Covered Entities also noted the challenges in assuring these steps are actually being taken.

As noted above, HITECH extended HIPAA's regulation directly to Business Associates. Some Covered Entities reported that HITECH's direct regulation of Business Associates did not enhance their confidence in Business Associate compliance while others felt Business Associate compliance would increase as a result. One Covered Entity said that direct regulation of Business Associates enhanced its comfort level because it was no longer solely responsible for enforcement of its Business Associate's privacy and security obligations. Another Covered Entity said that direct regulation of Business Associates made BAA negotiations easier because the law is now clear that Business Associates are responsible for complying with HIPAA regardless of whether they sign a BAA. Still other Covered Entities said that direct regulation of Business Associates made signing BAAs unnecessary: Business Associates have to comply with HIPAA regardless of whether they have signed a BAA with the Covered Entity, and most BAAs include only those provisions required by law. However, the Covered Entities interviewed did not all agree that the BAA requirements should be eliminated; a number still found BAAs worthwhile for the following reasons: they provide legal protections and recourse for both parties, they assign responsibility among the parties for different tasks, they address various business provisions not addressed by HIPAA, and they reinforce the need for confidentiality of important information. What's more, said one Covered Entity, they are "a fact of life." Health care stakeholders have grown accustomed to using them and it is not clear that eliminating the requirement for BAAs would necessarily reduce contracting obligations.

"Since HITECH, we have placed more emphasis on ensuring that our Business Associates understand their obligations with respect to their subcontractors. We also probe more closely into with whom our Business Associates share our PHI."

IV. Summary of Business Associate Interviews

a. HIPAA Compliance

Key Themes

- Large Business Associates generally have more resources and are better equipped to comply with HIPAA.
- Business Associates are challenged to track and comply with the varying terms of BAAs across multiple Covered Entities.
- Business Associates may experience "audit fatigue" and lack the staff and resources to support frequent audit requests; some larger Business Associates seek third party audits to try to satisfy the audit requests of their customers.
- Business Associates worry that small and solo physician practices are not prepared to comply with HIPAA and that downstream vendors sign BAAs without fully understanding their obligations under the Privacy and Security Rules.

Not surprisingly, larger Business Associates report fewer challenges in complying with HIPAA than smaller Business Associates. One large Business Associate reported the most difficult thing about HIPAA compliance is maintaining and updating thousands of BAAs. According to the Business Associate, eliminating the requirement for BAAs would free up resources to focus on "real" compliance, rather than updates and revisions to agreements. Small Business Associates also find BAAs to be a "pain point" because they are often subject to disparate requirements from multiple Covered Entity clients, and they struggle to track and comply with all of them. In contrast, large Business Associates are more likely to have sufficient bargaining power to dictate the terms of their business and legal agreements with Covered Entities. Further, if the Business Associate is a downstream subcontractor, they may get "stuck" with provisions that were adopted upstream and over which they have no control. For example, as noted above, some Covered Entities require shorter breach notification periods than are required under HIPAA and often include indemnification and liability provisions that are also not required under HIPAA. A number of Business Associates suggested that even greater standardization of BAAs could reduce compliance costs for all parties (although begging the question of whether such agreements should be needed if all provisions are standard).

Business Associates are challenged to find staff with HIPAA compliance and security expertise, especially compared to other, less "niche" positions within their organizations. Larger Business Associates may have the resources to recruit and hire staff with relevant background and experience, but smaller Business Associates end up relying on individuals with more general or IT–specific compliance knowledge, or completely outsourcing this function.

Business Associates are also challenged to comply with the number of audit requests they receive from Covered Entities. While the Covered Entities interviewed reported that they generally do not perform audits, Business Associates reported that they receive a significant number of audit requests related to their IT security, which require significant staff resources to address. Larger Business Associates would likely not have enough staff or resources to support audits by all of their Covered Entities. In an effort to get ahead of Covered Entities' audit requests, some Business Associates are completing third party audits and sharing these with Covered Entities with the goal of reducing Covered Entities' requests for more tailored or unique audits.

Business Associates that serve small or solo physician practices worry about the Covered Entities' compliance with HIPAA more so than their own. For example, Business Associates worry that small physician practices do not have appropriate technical safeguards in place and are at risk of breach. Other Business Associates worry their downstream vendors may not have appropriate safeguards in place or, if they are new or generally not part of the health care industry, may not truly understand their obligations under the Privacy and Security Rules but execute BAAs out of business necessity and/or fear of losing a business relationship.

For example, Aptible, a small software application developer and Business Associate, reported contracting with a vendor that provides a cloud application deployment platform that is designed to assist developers with HIPAA compliance. Among other things, the service has helped the Business Associate develop and document security risk analyses, as well as implement privacy and security policies and procedures (as required under the HIPAA Security Rule). The service also performs certain of the Business Associate's technical operations on its behalf, ensuring that they meet HIPAA's security requirements (e.g., that PHI is encrypted at rest and in transit). According to this Business Associate, which has only seven employees, working with this vendor has significantly reduced the heavy burden on innovative software companies that is otherwise associated with HIPAA compliance.

b. Training

Key Themes

- Training varies widely among Business Associates, with larger Business Associates more likely to offer established training and compliance programs.

A number of Business Associates are confident in their HIPAA compliance and reported a common theme of employee training. One Business Associate described its efforts beyond training to build a culture characterized by privacy and security, and, as a result, their employees take compliance seriously.

Most large Business Associates have established training and compliance programs, initiating training with new hire orientations and reinforcing components of the training through annual mandatory refresher courses and signs around the workplace reminding employees of their privacy and security obligations. Fewer Business Associates tailor their training based on employees' role (e.g., some employees may require more extensive training than others due to their access to PHI). Another Business Associate reported offering weekly web–based trainings to its workforce as well as an annual mandatory refresher course.

In contrast, smaller Business Associates may not offer any formal employee training, but may refer employees to standardized training and educational materials from OCR.

"In our organization, staff will call out their peers in the hallway if they are not complying with standard security protocols – for example, if they are not carrying the required credentials and identification."

V. Recommendations for Improving Compliance with HIPAA

a. Education and Training

Covered Entities and Business Associates alike suggested that Business Associates (particularly smaller companies) and smaller Covered Entities may benefit from additional education and training. For example, the average small provider practice is most concerned with caring for its patients and does not have the resources available to delve deeply into HIPAA compliance and the required risk assessments, trainings, etc. While OCR offers standardized education and training materials, some interviewees suggested that Business Associates and Covered Entities could benefit from more "user friendly" or "common sense" materials and/or education and training opportunities. Other interviewees, however, noted that there is a wealth of information available to assist Business Associates and Covered Entities in complying with HIPAA and that many Business Associates and Covered Entities are highly sophisticated and would not need additional education and training.

To this end, Covered Entities and Business Associates generally appeared willing to disseminate education and training materials within their organizations and also suggested that trusted trade associations or other government bodies would be an appropriate conduit for materials, webinars, and in–person trainings (e.g., county medical associations, colleges of physicians, California Medical Association, California Hospital Association). Many of these organizations already play a role in educating the health care industry and are "trusted" sources of information; they also have established communication networks allowing them to reach broad audiences of Covered Entities and Business Associates without "starting from scratch."

"Training modules should be comprehensive and authoritative so that Business Associates can deploy the information to their staff. There should be a go–to person/resource for follow up questions."

In California specifically, Covered Entities identified the need for additional education and training for Business Associates around breach notification, including California's heightened breach notification requirements. As discussed in this report, Business Associates that are less sophisticated, smaller, or new to health care are often unaware of California's breach notification requirements and push back on BAA provisions designed to comply with these requirements. Covered Entities also noted Business Associates may benefit from education about California's protections for behavioral health, mental health, and other sensitive health information. Today, Covered Entities generally do not provide training to their Business Associates and lack the bandwidth and desire to do so. Many Covered Entities also voiced concern about the liability they might incur as a result of taking on the responsibility for training a Business Associate's workforce on HIPAA compliance.

Some Business Associates also identified the lack of a collaborative culture or community to assist other Business Associates in sharing best practices and information relative to HIPAA compliance due to competitive interests. As a result, some Business Associates felt left on their own searching for resources and guidance and sometimes recreating the wheel. Establishing and publicizing a "go to resource" for these Business Associates could avoid duplication of effort and increase standardization. Those Business Associates who felt more confident in their HIPAA compliance capabilities discounted the need for this type of resource.

b. Voluntary Third Party Certification

During the interviews, some (though decidedly not all) Covered Entities and Business Associates suggested that an outside/third–party certification process for Business Associate compliance with HIPAA could be helpful. The voluntary certification process would serve to ensure that Business Associates continuously meet some minimum or baseline level of HIPAA compliance (e.g., annually) so that Covered Entities can be confident engaging Business Associates without performing a significant amount of due diligence. If widely accepted by Covered Entities, a voluntary third party certification process could also potentially save Business Associates time and resources as it might reduce the due diligence/audit/questionnaire requests they receive from Covered Entities.

Such a certification process is emerging or exists to some degree in the market. There are a variety of standards and certification bodies that offer relevant information security certifications, yet none are widely accepted as the "gold standard" by Covered Entities or Business Associates. One certification entity which currently offers healthcare specific self–assessments and certifications for Business Associates has seen increased interest and adoption among health plans, pharmaceutical companies and large health care providers since the passage of HITECH.

While many interviewees were supportive of this idea, they recognized the challenges with both developing a certification process that would broadly meet the industry's needs while also being stringent enough that it would be widely accepted by both Covered Entities and Business Associates. What standards would be the basis for certification (e.g., national or state)? How would the certification achieve sufficient adoption so that it would be cost effective to engage in the process? These questions may need to be resolved through a collaborative industry–wide process. If resolved, a certification process could help relieve the sense of "audit fatigue" felt by some Business Associates and Covered Entities and potentially provide more certainty in the marketplace.

However, some Covered Entities, especially larger Covered Entities, noted that they would be unlikely to accept a third party certification in lieu of their existing due diligence and oversight processes. While they would be open to using the certification as a screening tool, the impact of potential HIPAA violations is significant enough that they would prefer to maintain control and oversight of their Business Associates. Other Covered Entities concurred, noting that it is unclear whether a third party certification process would be able to address the priorities of the various government agencies that may be involved in the event of a breach (e.g., the Centers for Medicare and Medicaid Services, the Department of Health Care Services (Medi–Cal), Covered California (Health Insurance Marketplace), the Department of Managed Health Care, and the State Attorney General). Further, at least one Business Associate was adamantly opposed to the idea, arguing that third party certification processes rarely meet the high expectations that are placed on them and instead impose significant burdens on those subject to evaluation.

Third Party Assessments

- Statement on Standards for Attestation Engagements (SSAE) No. 16, developed by the American Institute of Certified Public Accountants, Inc., addresses organizational controls relevant to entities' financial reporting, IT and related processes.[34] The SSAE No. 16 replaced the Statement on Auditing Standards (SAS) No. 70, which was a widely recognized auditing standard.
- The Health Information Trust Alliance (HITRUST) developed a common security framework that "harmonizes the requirements of existing standards and regulations, including federal, third party, and government."[35] Today, Covered Entities and Business Associates can perform assessments against the healthcare specific framework and receive a certification that may in turn be shared with relevant parties.
- The International Organization for Standardization (ISO), the largest developer of voluntary international standards, developed a set of standards focused on information security management known as the ISO 27001.[36] Organizations may be certified to ISO 27001 by third party certification bodies (ISO does not perform certification).

The Electronic Healthcare Network Accreditation Commission (EHNAC) is a standards development and accrediting body. EHNAC offers certification of organizations' regulatory compliance with HIPAA, HITECH, ARRA, and the Affordable Care Act.[37]

c. Other Strategies to Improve Compliance

Detailed below are other strategies and themes that emerged regarding how to improve understanding of and compliance with HIPAA.

- Standardization: Many Covered Entities and Business Associates were supportive of greater standardization to minimize the burden of HIPAA compliance on their limited staff. Particular opportunities for standardization include BAAs, due diligence/risk assessments/questionnaires, and independent audits/certifications.

- Development of assessment tools: Several Covered Entities suggested they would be interested in purchasing a tool to evaluate and manage Business Associates. Covered Entities noted that vendors would need to tailor their products to meet California requirements that go above and beyond HIPAA. One Business Associate noted that Business Associates that are confident in their knowledge of and compliance with HIPAA could benefit from a tool that helps them protect themselves against Covered Entities that attempt to take advantage of Business Associates by shifting certain obligations and costs to Business Associates. For example, a tool that helps Business Associates identify common BAA provisions that are mandated by HIPAA versus those that are not (and to which the Business Associate need not agree), could be helpful in this regard.

- Auditing for compliance: Today, Covered Entities typically only have resources to audit the top tier of Business Associates that pose the greatest risk, if they are performing audits at all. Some Covered Entities would welcome resources to perform increased audits to ensure Business Associate compliance. Short of providing Covered Entities with resources to increase their audit capabilities, educating Covered Entities about the importance of asking their Business Associates to provide copies of security risk analyses may lead to more Business Associates conducting assessments. Tools and services to help small, technology–focused Business Associates, such as software application vendors, comply with HIPAA, including its audit requirements, exist in the market today and are likely to become increasingly important for start–ups and small Business Associates.

- Guidance for software application developers and other cloud–based vendors that are generally new to health care and HIPAA: As discussed earlier in the paper, cloud–based vendors are a class of Business Associates that are generally new to HIPAA and may not understand their obligations under federal and state health privacy laws. Covered Entities sometimes struggle in their negotiations with cloud–based vendors because the vendors may not identify as a Business Associate or want to comply with the terms of a BAA. Given that some cloud–based vendors are relatively new to the health care market, they could benefit from explicit guidance and materials outlining their obligations under HIPAA and pointing them to education and training resources or to vendors that provide "HIPAA compliance as a service" as described above.

  Similarly, the industry should consider opportunities to develop a workforce that is knowledgeable about HIPAA and "match" such a workforce with some Business Associates (e.g., emerging technology companies) that otherwise may have challenges recruiting for HIPAA compliance roles. With the growing technology boom, professional and training programs, such as those offered by universities and community colleges, may consider expanding their scope and coursework to include privacy and security compliance expertise.

- Education about who is – and who is not – a Business Associate: Covered Entities and Business Associates acknowledged that Covered Entities are generally taking an overly cautious approach relative to their Business Associates and BAAs (e.g., Covered Entities signing BAAs with other Covered Entities for disclosures for treatment purposes). This is due in part to confusion regarding which organizations qualify as Business Associates as well as a lack of resources to individually assess and appropriately classify each vendor. Education or training modules with clear examples/use cases of what organizations are considered Business Associates and when a Covered Entity should enter into a BAA may help reduce some of the confusion and general BAA fatigue in the marketplace.

- Compliance Officer Peer Network: One of the interviewees shared their experience participating in a "Compliance Officer Peer Network" with similar provider organizations and found this training and peer learning network to be helpful for purposes of educating Covered Entities about their responsibilities and disseminating best practices. The network made its trainings and materials available via the web to network members as well as to the public for a fee. Similar Business Associate–focused networks could be established with the goal of sharing lessons learned as well as identifying opportunities for greater standardization across the industry. Interviewees generally agreed that the generic training materials available to Business Associates through OCR are too vague to be helpful; some Business Associates expressed the need for examples of how other, similarly situated Business Associates have implemented processes to comply with HIPAA.

- Policymakers should consider whether BAAs are really necessary: Several Business Associates and Covered Entities argued that because Business Associates are now directly regulated under HIPAA, there is no need for BAAs, which generally focus on standard provisions, and typically only set forth the Business Associates' security obligations

and do not delineate the specific uses and disclosures the Business Associate may make under the BAA (something that is more likely to be covered in the underlying services agreement). At least one Covered Entity disagreed, however, arguing that it needs the BAA in order to obligate the Business Associate to comply with requirements (such as shorter breach notification time periods) that go above and beyond the minimums set out by HIPAA.

VI. Conclusion

Business Associates and Covered Entities play key roles in the delivery of health care, but many struggle with HIPAA compliance as they focus the majority of resources on their core businesses and caring for patients. While there are many highly sophisticated Business Associates and Covered Entities that do not think they need additional training or education on HIPAA compliance, others felt they could benefit from it. Notably, smaller organizations with limited resources often seek out publicly available materials, and these are often too general or not user friendly. As the health care industry continues to grapple with the best approach to oversight of Business Associate compliance with HIPAA, some are considering how a third party certification process may ease the burden on Business Associates and Covered Entities while also setting a "gold standard" that is acceptable to Covered Entities across the country. Lastly, there is growing demand in the market for standardization of BAAs as well as innovative tools and services to help small and new Business Associates understand and comply with HIPAA. Actions like those described above could promote increased awareness among Business Associates (and Covered Entities) of their obligations under HIPAA, ultimately leading to a broader culture of awareness and compliance.

Appendix A
Covered Entity Interview Guide

I. Use of Business Associates

(a) How many business associates (BAs) do you have today (roughly)?

(b) For what types of activities do you use BAs?

(c) Give us a sense of the approximate size of the BAs you typically use – what percentage are small (fewer than 25 employees), mid–size (25–100) and large (more than 100 employees)?

(d) If relevant, please describe which types of BAs (small or large, etc.) provide which types of services.

(e) How would you describe the range of sophistication of your BAs when it comes to the Health Insurance Portability and Accountability Act (HIPAA)?

II. Investigating BAs: Due Diligence

(a) How much (if any) due diligence do you perform on BAs with respect to compliance with HIPAA?

(b) What impacts whether or not you engage in any due diligence of BAs with respect to HIPAA? To what extent have you changed your approach to evaluating BAs for HIPAA compliance following the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act?

(c) If you do perform due diligence, what do you focus on? Do you do any of the following things before signing a business associate agreement (BAA)?

(i) Reference checks with other consumers

(ii) Review of Office for Civil Rights (OCR) website on breaches

(iii) Media search

(d) Litigation search

(i) Review of 10–k (for public companies)

(e) Questionnaire on privacy and security practices

(f) Review of key privacy and security documents and/or commission of third–party validation of policies and procedures

(1) Policies and procedures

(2) Security risk analysis

(3) Contingency plan

(g) What are the warning signs you think should tip a covered entity (CE) off not to engage with a BA (i.e., that the BA is probably unable to comply with HIPAA's requirements)?

III. Experiences Working with BAs

(a) BA Personnel

(i) Do you interact with BA personnel? If so, with whom do you typically work at each BA (e.g., their general counsel? compliance officer? others?)? Do you find that you work closely with this person on an ongoing basis – why or why not? Does this vary by size of BA and/or type of activities engaged in by the BA?

(ii) Do your BAs typically have a privacy or compliance officer – and is this information you try to obtain in advance of entering into a BA relationship?

(b) Negotiations with BAs

(i) Please tell us about your experiences negotiating BAAs with your BAs. Do they engage you in negotiations with respect to HIPAA compliance–related issues? If so, which issues are commonly raised in negotiations, and what are the typical results of those discussions?

(c) Oversight of BA Compliance

(i) To what extent do you get involved in overseeing or managing a BA's compliance with HIPAA? If there is involvement, what triggers such oversight/management – and what does it typically involve?

(ii) Do you track your BAs and BAAs agreements – and if so, what types of information do you maintain about BAs and BAAs, and what (if any) oversight do you perform to keep this up–to–date? Post–HITECH, are you more or less likely to do such tracking?

(iii) What are the top weak spots for BAs?

(d) Can you share any lessons you have learned with respect to working with BAs?

(e) Breaches Involving BAs

(i) Can you share any lessons learned with respect to working with a BA in response to a breach? What have you found most challenging (e.g. complying with various state and federal breach reporting timelines)?

(f) Restrictions on How BAs Handle/Use PHI

(i) Do you allow your BAs to maintain protected health information (PHI) offshore? Why or why not?

(ii) Do you allow your BAs to use de–identified data for commercial purposes? How frequently is this an issue in negotiating BAAs?

(iii) Who makes the determination of whether to return or destroy PHI at the end of the BA–CE relationship? Is this typically covered by the BAA – and, if so, how frequently is it honored?

(g) Do you find that BAs comply with their obligations to inform you of subpoenas or other legal requests for protected health information (PHI) and cooperate in resisting requests (due to state law implications)?

(i) Do you find that BAs comply with any (possible) obligations to respond directly to access, amendment, accounting and restriction on use requests? Are these activities that you customarily task to BAs?

(h) Do you find that BAs comply with any (possible) obligations to obtain patient consent to the extent legally required?

(i) Have you ever/would you consider/what do you think of the idea of performing audits of your BAs? Do you contractually require your BAs to perform audits themselves and report the results to you?

IV. HITECH Questions

(a) Do you find the new distinctions in relation to who is a BA (i.e., entities that transmit (but do not maintain) PHI and do not routinely access PHI) easy or challenging to put into practice?

(b) Are you seeing BAs comply with the requirement that they enter into BAAs with their subcontractors? Are you asking to see those BAAs and/or keep them on file?

(c) Does the fact that BAs are now directly subject to HIPAA make you feel more confident about their performance? Why or why not?

V. Strategies for Educating Business Associates about Better HIPAA Compliance

(a) What do you think are the biggest barriers to BA compliance (e.g., funding, knowledgeable employees)?

(b) What are the five things you would encourage other CEs to do to improve their management of their BA's compliance with HIPAA?

(c) What are five things you would encourage BAs to do to improve their compliance with HIPAA?

(d) We have heard some CE representatives speak of the need for an outside/third–party certification process for BAs (i.e., to ensure they meet some minimum level of HIPAA compliance so that CEs can be confident engaging with them). What do you think of this idea?

(e) How can a BA properly educate/train its workforce to ensure compliance and protect against breaches?

Appendix B
Business Associate Interview Guide

I. General Characteristics of Organization

(a) What services does your organization provide to covered entities (CEs)?

(b) How many CEs do you work with right now?

(c) How many employees to do you have?

(d) Do you have a privacy or compliance officer? If not, who has responsibility for complying with your business associate agreements (BAAs)/Health Insurance Portability and Accountability Act (HIPAA)?

(e) Do you face challenges in recruiting employees with HIPAA expertise and, if so, can you please describe them? Do you consider recruiting employees with HIPAA Expertise a priority?

II. Compliance with HIPAA

(a) What aspects of complying with HIPAA do you find most challenging and why?

(b) What aspects of complying with HIPAA do you find easiest and why?

(c) Tell us about the policies and procedures you have in place to comply with HIPAA (e.g., performance of risk assessments, use of security measures). Can you share any policies and procedure documents with us?

(d) Do you train your employees on HIPAA compliance? Can you tell us about your training program and/or share your materials?

III. Strategies for Educating BAs about Better HIPAA Compliance

(a) If you could have help in the form of additional funding for complying with HIPAA, how much would you need? What would you use it for?

(b) If you could get help from your CE clients in terms of complying with your BAA and HIPAA, would you want it? What could they do that would be most helpful?

(c) Would you accept help from a third party (e.g., a foundation) and what type of help would be most useful?

[1] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at Title XI of the Social Security Act).

[2] The report was also informed by a literature review that included analysis of (i) enforcement actions by government agencies with authority under HIPAA and state privacy laws; (ii) private lawsuits by individuals affected by HIPAA or state privacy law violations; (iii) government-compiled HIPAA breach statistics; (iv) trade press accounts of large-scale HIPAA breaches involving Business Associates; and (v) government-released audit findings of Covered Entities' compliance with HIPAA.

[3] Pub. L. 111–5, 123 Stat. 115 (Feb. 17, 2009).

[4] 45 CFR § 160.103.

[5] 45 CFR § 164.524.

[6] 45 CFR Part 164.

[7] 45 CFR § 160.103.

[8] 78 Fed. Reg. § 5571–5574 (January 25, 2013).

[9] 45 CFR § 160.103.

[10] 75 Fed. Reg. § 40,868 and 40,872 (July 14, 2010).

[11] 45 CFR § 160.103.

[12] 45 CFR §§ 164.103, 165.502(e) and 165.504(e).

[13] HITECH § 13404.

[14] HITECH § 13401.

[15] HITECH §§ 13410, 13411.

[16] See, e.g., Health Information Security and Privacy Collaboration (HISPC), Report on State Law Requirements for Patient Permission to Disclose Health Information. August 2009. Available at http://www.healthit.gov/sites/default/files/disclosure-report-1.pdf.

[17] 45 C.F.R. Part 160, Subpart B.

[18] California Civil Code §§ 56–56.37.

[19] California Civil Code §§ 56.35–36.

[20] 65 Fed. Reg. 82,504-05 (Dec. 28, 2000); HHS OCR, "Business Associates" available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html. Last accessed July 24, 2014.

[21] Id.

[22] Id.

[23] HITECH clarified that Covered Entities could be held responsible for the acts of any Business Associates who were acting as "agents" of those entities (versus independent organizations). 45 CFR § 160.402(c)(1).

[24] 45 CFR § 164.402.

[25] 45 CFR § 164.404.

[26] California Civil Code §§ 1798.82 and 1798.29; California Health and Safety Code § 1280.15.

[27] California Health and Safety Code § 1280.15.

[28] Id.

[29] California Civil Code § 1798.82(a).

[30] 45 CFR §§ 164.502(d)(2), 164.514(a) and (b).

[31] 45 CFR § 160.103.

[32] 45 CFR §§ 164.504(e),164.314.

[33] 45 CFR § 160.103.

[34] American Institute of CPAs, "Statements on Standards for Attestation Engagements," http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx.

[35] Health Information Trust Alliance, "About Us," http://hitrustalliance.net/about-us/.

[36] ISO, "ISO/IEC @7001 – Information security management," http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[37] EHNAC, "EHNAC Overview," https://www.ehnac.org/about/.