OMNIBUS RULE IMPLICATIONS FOR LAW FIRMS AS BUSINESS ASSOCIATES

Sarah S. Murdough, Esq.
Sulloway & Hollis
smurdough@sulloway.com
(603) 224-2341

Holly S. Bell, Esq.
Norman, Wood, Kendrick & Turner
hbell@nwkt.com
(205) 328-6643

Lisa H. Leiner, Esq.
Dannel C. Duddy, Esq.
Harman, Claytor, Corrigan, Wellman
lleiner@hccw.com
dduddy@hccw.com
(804) 747-5200

Mary G. Pryor, Esq.
The Cavanagh Law Firm
mpryor@cavanaghlaw.com
(602) 322-4000

Michael P. Scott-Kristansen, Esq.
Hurwitz & Fine
MPS@hurwitzfine.com
(716) 849-8900

I. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) was passed on August 21, 1996, with the stated goals of making health care delivery more efficient and increasing the number of Americans with health insurance coverage. The Act sought to accomplish these goals through three main provisions: (1) information portability provisions, (2) tax provisions, and (3) administrative simplification provisions. The third provision called for the Secretary of Health and Human Services (HHS) to issue regulations regarding the electronic transmission of health information. However, Congress also feared that the increasing use of electronic transmissions could negatively affect patient privacy. As a result, Congress mandated in HIPAA that nationwide security and privacy standards be enacted to protect health information—the Security Rule and the Privacy Rule. HIPAA also established penalties for privacy and security violations–the Enforcement Rule.

The Security Rule and Privacy Rule originally applied only to covered entities—health plans, health care clearinghouses, and certain health care providers. In addition, recognizing that these entities often use consultants, contractors, or other entities to accomplish their activities, the Privacy Rule allows for the sharing of certain information with "business associates." Protected Health Information (PHI) may only be shared with a business associate if the covered entity obtains satisfactory assurances that the business associate will use the information only for the business purpose for which it was disclosed and will implement appropriate security measures to protect that information.

In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the larger American Recovery and Investment Act. HITECH provided funds (to be later replaced by fines) and updated policy to encourage health care providers to adopt and make meaningful use of Electronic Health Records (EHR). However, Congress still had privacy and security concerns regarding electronic patient information and gave HHS broader jurisdiction and increased power to punish covered entities and business associates for failures to securely handle patient information. HITECH also expanded the definition of a "business associate" to include certain organizations, such as health information exchange organizations, regional health information organizations, or e-prescribing gateways, that require routine access to PHI despite the fact that they are not, strictly speaking, engaged in a traditional business relationship with the covered entity.

Pursuant to HIPAA and HITECH, HHS issued a number of interim regulations and rules regarding the protection of personal health information, including a requirement for the reporting of any breach of PHI security or privacy to HHS and the affected individual. These interim regulations were called the "Interim Final Rule" (IFR). On January 17, 2013, HHS issued final rules that will require additional compliance efforts by September 23, 2013, with steep penalties for non-compliance. These rules are collectively known as the "Omnibus Rule" due to the large number of topics and regulations they cover. However, in particular, the Omnibus Rule changes the definition of a business associate and clarifies how business associates may be directly liable for compliance with the Security Rule and Privacy Rule. The Omnibus Rule also changes the breach notification standard from one requiring notification only where there is "significant risk of harm" to one that begins with a presumption of breach and, therefore, requires notification

unless the covered entity or business associate can establish a low probability of harm. Furthermore, the Omnibus Rule specifically addresses disclosure requirements in certain specialized situations, such as when an individual has been deceased for over 50 years or when the individual is a student. These issues, in addition to potential penalties, are discussed below.

II. Business Associates and Business Associate Agreements

A. Business Associates

A business associate is an entity that, on behalf of a covered entity, performs functions, activities, or services involving the use or disclosure of protected health information. Accordingly, law firms performing functions, activities, or services involving the use or disclosure of PHI "on behalf of a covered entity" fall squarely within the definition of business associate. In light of the changes that will be addressed in this publication, it is critical for law firms to be informed and in strict compliance with the Omnibus Rule. The Omnibus Rule expanded the definition of "business associates" to include those persons who, other than in the capacity of a workforce member of the covered entity, create, receive, *maintain* or transmit PHI on behalf of the covered entity. One important change that law firms as business associates must be aware of is the addition of "subcontractors" to the definition of business associates. 78 Fed. Reg. at 5573.

A "subcontractor" is "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate" and "that creates, receives, maintains, or transmits [PHI] on behalf of the business associate." The inclusion of subcontractors in the definition of a business associate and the addition of direct liability for business associates compels law firms to seriously analyze which relationships qualify the firm as a business associate and how the firm will achieve compliance with the Omnibus Rule. Does your law firm use a data storage company? A shredding service? An iCloud service provider? What about disclosure of PHI to expert witnesses? The analysis of whether a subcontractor is a business associate is the same analysis applied to whether a covered entity's contractor is a business associate.

It is also important to note two things. One, the lack of a contract between the parties does not prevent a "subcontractor" designation. Two, the "subcontractor" designation can extend through a chain of relationships for an infinite number of degrees. If a subcontractor delegates or outsources any of their services, activities, or functions to other subcontractors, those subcontractors also become business associates. It does not matter how far down the chain the information flows; all contractors and subcontractors are business associates if they create, receive, maintain, or transmit PHI. 78 Fed. Reg. at 5572-5574.

Although the Omnibus Rule recognizes the "conduit exception," HHS cautioned that the exception is intended to be narrow and exclude only those entities providing mere courier services. "[A] conduit transports [protected health] information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law." 78 Fed. Reg. at 5571. A determination of which types of data transmission services are "business associates" versus "mere conduits" will be dependent upon the nature of

the services provided and the extent to which the entity needs access to PHI to perform its service for the covered entity (or business associate in the case of potential subcontractor conduits).

B. Examples of Entities Qualifying as Business Associates/Subcontractors

- Data storage company that has access to a covered entity's PHI (whether digital or hard copy) even if the data storage company does not view the PHI or only does so on a random or infrequent basis. 78 Fed. Reg. at 5572.
- Company hired by business associate to handle document and media shredding for the secure disposal of paper and ePHI. 78 Fed. Reg. at 5573.
- Law firms that require access to PHI in order to perform a service for a covered entity, such as representation in medical malpractice actions in which the PHI of patient/plaintiff is necessary and obtained directly from the client/covered entity.

C. Examples of Entities Not Qualifying as Business Associates/Subcontractors

- A telecommunications company with occasional, random access to PHI when reviewing whether the data transmitted over its network is arriving at its intended destination. 78 Fed. Reg. at 5571-5572.
- A company providing transmission services (whether digital or hard copy), including any **temporary** storage of transmitted data incident to such transmission. 78 Fed. Reg. at 5572.
- U.S. Post Office. 78 Fed. Reg. at 5571.
- United Parcel Service. 78 Fed. Reg. at 5571.
- Internet service providers (ISPs). 78 Fed. Reg. at 5571.
- Company hired by business associate to handle the shredding of documents and media pertaining to the business associates own management, administration, or legal responsibilities and not related to the business associate's responsibilities to the covered entity. 78 Fed. Reg. at 5573.

D. Business Associate Agreements

Covered entities are required to have a written agreement with their business associates that complies with the regulations, but are not required to enter into Business Associate Agreements (BAAs) with the subcontractors of its business associates. The business associate must execute and have in place BAAs with its subcontractors. *See* 45 C.F.R. 164.502(e)(1). Section 164.504(e) sets forth in detail the specific requirements for BAAs. Sample provisions for a BAA have been published on HHS' website at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html. Thus, law firms as business associates must have BAAs in place with covered entities and with its "subcontractors." Although business associates are required by law to have a BAA with their subcontractors, covered entities may require that business associates do so in their BAA with the business associate. A business associate is not in compliance with the Omnibus Rule "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 C.F.R. 164.504(e). The Omnibus Rule provides for increased penalties for noncompliance and potential liability for business associates based on the acts/omissions of their subcontractors under an agency theory. *See* 45 C.F.R. 160.402(c). Therefore, consideration should be given to provisions in BAAs that address indemnification. It is also critical that business associates educate their subcontractors and bring them in the loop on the new requirements and potential liability and penalties. Subcontractors may be resistant to executing a BAA, but it is a requirement and now business associates can be held directly liable for failure to do so.

The Omnibus Rule provides potentially for a longer period of time to comply with BAA requirements. Compliant BAAs entered into before January 25, 2013, that are not modified between March 26 and September 23, 2013, will be deemed compliant under the Omnibus Rule until either they are renewed or modified or September 22, 2014, whichever is earlier. BAAs that are entered into or renewed before September 23, 2013, must comply with the Omnibus Rule by September 23, 2013.

III. Breach Notification

The Omnibus Rule also modified the IFR governing breach notifications issued on or before August 24, 2009. Compliance with the now-designated "Final Breach Notification Rule" is required by September 23, 2013. The Final Breach Notification Rule makes some significant changes to the definition of a breach and the risk assessment approach. These changes impact the obligations of covered entities to report breaches to individuals, the media and/or HHS, and the obligations of business associates to notify covered entities of breaches to enable covered entities to make appropriate notifications.

A. Presumption of Breach and the Low Probability Standard

The Final Breach Notification Rule makes clear that an impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach that requires notification, unless there is a "low probability" that the PHI was compromised (or one of the exceptions, discussed below, applies). The "low probability" standard replaces the IFR's "risk of harm" standard, which had afforded covered entities and business associates greater discretion in determining whether to issue breach notifications. Covered entities and business associates must now overcome a presumption that any breach requires notification and must examine the following four factors to determine whether notification is required:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who impermissibly used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk has been mitigated.

Other factors may also be assessed in order to evaluate the overall probability that the PHI was compromised. If the assessment fails to show a low probability of compromise, breach notification is required in accordance with the breach regulations. Commentary to the Final Breach Notification Rule also notes that a covered entity may choose to notify individuals without completing the above risk assessment. *See* 78 Fed. Reg. at 5643. That commentary also suggests that it will be the rare occasion where notification is not warranted. *See* 78 Fed. Reg. at 5642-5643. HHS anticipates publishing future guidance on performing risk assessments in frequently occurring scenarios. 78 Fed.Reg. at 5643.

B. Limited Data Sets and Exceptions to "Breach"

HHS has also narrowed the list of uses or disclosures excepted from the definition of "breach." Previously, under the IFR, there were four categories of breach exceptions. In particular, the IFR excepted the impermissible use or disclosure of a limited data set that did not include dates of birth and ZIP codes. The Final Breach Notification Rule removes this exception. Therefore, any impermissible use or disclosure of a limited data set is now subject to risk assessment to determine if there is a low probability that the PHI has been compromised. The other three exceptions to "breach" remain as follows:

1. Unintentional, good faith, acquisition, access, or use of PHI by a workforce member or person acting under the authority of the covered entity or business associate;

2. Inadvertent disclosure of PHI from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate; and

3. A good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

C. Other Changes

HHS made no significant changes to the breach notification procedure, but Commentary to the Final Breach Notification Rule does offer the following significant clarifications:

- Individuals receiving highly confidential treatment services may receive breach notification orally where the individual has requested to receive verbal communications so long as they are advised to pick up a written breach notice directly from the provider. 78 Fed. Reg. 5651.

- Individuals whom a medical provider believes may sustain substantial harm by receiving breach notification must still be notified; however, they may be called first to receive notice directly before written notice is mailed if such oral notice will not delay the timeliness of the notice. 78 Fed. Reg. 5651.

- Notifications to the Secretary for breaches affecting less than 500 individuals must be provided to HHS within 60 days after the end of the calendar year in which the breach was *discovered*, not the year in which the breach occurred. 78 Fed. Reg. 5654.

D. Documentation, Policy and Procedures, and Compliance Date

Compliance with the new breach notification risk assessment is required by September 23, 2013. Until then, covered entities and business associates must comply with the IFR, but the changes to the breach notification standards outlined above will require covered entities and business associates to update their policies and procedures and train employees on those changes during this transition period. Of course, documentation of all risk assessments to support the reasonableness of breach notification determinations as well as documentation that notifications were made is key to ensure continued compliance.

IV. Security Rule and Privacy Rule Changes

The most significant change to the Security and Privacy Rules (the "Rules") is that they now apply directly to business associates. Law firms, therefore, will be obligated to achieve compliance with substantially the same HIPAA rules as their clients. Although the Omnibus Rule purports to limit the applicability of the Security and Privacy Rules to business associates to "where provided," as a practical matter, business associates must comply with the entirety of the Security Rule and most of the Privacy Rule provisions that apply to covered entities.

A. Direct Liability of Business Associates Under the Security Rule

The general Security Rule is comprised of several parts: the general requirements, the standards, and the implementation specifications. The general requirements are very general, the standards are more specific, and the implementation specifications are the most specific, containing instructions for how to comply with the standards. This section will provide a global overview and permit issue spotting.

i. The general requirements

The general requirements of the Security Rule, 45 C.F.R. § 164.306, provide that business associates must ensure the confidentiality, integrity, and availability of all electronic PHI (ePHI) they handle; protect against reasonably anticipated threats to the security and integrity of such information; protect against any uses or disclosures that are not permitted under the Privacy Rule; and ensure their workforce members comply with the Security Rule. The business associate may use any security measures that reasonably and appropriately achieve the requirements of the Security Rule, taking into consideration its own size and technical capabilities, the probability and severity of risk to ePHI, and the cost.

ii. The Standards

There are five different categories of standards explored below. Each category of standard has its own implementation specifications. We have treated these requirements collectively for the purpose of simplicity.

Administrative safeguard standards focus on personnel and administrative matters. 45 C.F.R. § 164.308. There are eight standards under this category, requiring everything from conducting risk analysis and minimization to appointing an official responsible for Security Rule compliance. This safeguard also contains the requirement that covered entities and business associates get adequate assurances from their business associates, meeting the requirements for BAAs as set forth under the organizational requirement standards. 45 C.F.R. § 164.308(b).

Standard 1: Implement policies and procedures to prevent, detect, contain, and correct security violations, including:

- Assessing and addressing potential risks to and vulnerabilities of ePHI in the entity's possession,
- Adopting a sanction policy for workforce members who fail to comply with security policies, and
- Regularly reviewing activity on IT systems.

Standard 2: Designate a security official responsible for achieving compliance with the Security Rule.

Standard 3: Ensure only workforce members who are authorized to access ePHI under the Privacy Rule have access by authorizing, supervising, and terminating access.

Standard 4: Establish policies to limit access to ePHI to those instances and circumstances prescribed by the Privacy Rule, including policies for granting access to workstations, transactions, programs, or processes containing ePHI.

Standard 5: Provide security training to all workforce members, create passwords, monitor log-in attempts, and address security breaches (including malicious software).

Standard 6: Establish procedures for identifying, responding to, mitigating, and documenting security incidents.

Standard 7: Establish emergency response procedures (such as for fire, vandalism, natural disaster, or system failure), including those for data backup and recovery and the continuation of ePHI protection processes.

Standard 8: Perform both technical and nontechnical evaluations of the extent to which policies and procedures meet the requirements of the Security Rule.

Physical safeguard standards require more than just lockable doors. 45 C.F.R. § 164.310. Business associates must control and prevent unauthorized physical access to their facility and electronic information systems. There are four standards under this category.

Standard 1: Control facilities and electronic information systems so only those who are properly authorized have access. These controls must:

- Allow access for the purpose of restoring lost data and conducting emergency operations,
- Prevent physical access to, theft from, or tampering with facilities or equipment where ePHI is held, and
- Document modifications to walls, doors, locks, and other physical security components.

Standard 2: Control the environment where workstations are found and the functions performed at such workstations.

Standard 3: Physically safeguard workstations that access ePHI.

Standard 4: Control the handling of electronic media that contains ePHI, including computers and their hard drives. Handling includes disposal, reuse, and movement.

Technical safeguard standards focus on limiting access to ePHI through technical and software-based measures. 45 C.F.R. § 164.312. One detail worth noting here is that some degree of digital security expertise will be required because the business associate must not only restrict people and entities from accessing ePHI, but also restrict unauthorized programs from accessing ePHI. Entities have an affirmative obligation under the Security Rule to prevent software and internet applications from inappropriately accessing ePHI. There are five standards under this category.

Standard 1: Control access to systems containing ePHI by persons and programs. Controls include unique usernames, automatic logoffs, encryption, and decryption. Controls must also permit emergency access to ePHI.

Standard 2: Install mechanisms, including software, that record activity in information systems that contain ePHI.

Standard 3: Install mechanisms that verify whether ePHI has been altered or destroyed.

Standard 4: Install mechanisms that verify whether the person seeking access to ePHI is the person claimed.

Standard 5: Protect ePHI as it is transmitted through an electronic network by installing mechanisms that encrypt ePHI where appropriate.

The *organizational requirement* standards focus on what is required for business associate agreements and a business associate's agreements with subcontractors. 45 C.F.R. § 164.314. This is discussed in greater detail throughout this article.

Policies and procedures standards require the adoption of reasonable and appropriate policies to comply with the Security Rule. 45 C.F.R. § 164.316. The policies may be changed at any time, but the changes must be documented. Such documentation must be preserved for six years. Because the term reasonable sometimes connotes a certain degree of error, the standards also state that the reasonable and appropriate standard does not excuse violations of the Security Rule. A covered entity's or business associate's *goal* should be perfection.

B. Direct Liability of Business Associates Under the Privacy Rule

Previously, the prohibitions and mandates of the Privacy Rule only applied directly to covered entities. Now, they also apply directly to business associates. 45 C.F.R. § 164.502. While the Security Rule requires procedures, policies, and practices that protect ePHI, the Privacy Rule states which disclosures and uses of PHI are permissible or required. The Privacy Rule, like the Security Rule, contains general rules, standards, and implementation specifications; however, our focus here will be narrower.

i. Required and Permissible Uses and Disclosures

Predictably, required and permissible uses and disclosures by business associates are closely linked to those uses and disclosures that are required or permitted for covered entities. Business associates may use or disclose PHI only where it is both required by law and required or permitted by its BAA. 45 C.F.R. § 164.502(a)(3). If a use or disclosure of PHI would be prohibited for covered entities, the business associate also may not use or disclose PHI in that manner. This means law firms and other business associates are going to have to know not only what is required or permitted in their BAA, but also what disclosures are required directly by law. There is an exception to the rule for permissible uses of disclosures for business associates where it is for their own proper management and administration.

A business associate's *required* uses or disclosures, at least, are somewhat simpler. Business associates must disclose PHI (1) to allow the Secretary of HHS

to investigate whether the business associate is compliant with the Omnibus Rule, and (2) to a covered entity, an individual, or an individual's designee where it is necessary to satisfy a covered entity's obligation to provide ePHI in the electronic form requested or to a party designated by the individual. 45 C.F.R. § 164.502(a)(4).

ii. The Minimum Necessary Standard

The Minimum Necessary Standard is part of the Privacy Rule's General Rules and is rightfully regarded as a key requirement of the Privacy Rule. The actual change to the statutory text is quite simple and only makes the standard, which existed under the previous regulations, applicable to business associates as well as covered entities. The standard now requires business associates and covered entities, when using or disclosing PHI or requesting PHI from another business associate or covered entity, to "make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." 45 C.F.R. § 164.502(b)(1).

There are six exceptions to the Minimum Necessary Standard. 45 C.F.R. § 164.502(b)(2). Summarily, these exceptions are limited to where the disclosure is made to the individual, to a health care provider for treatment, to the Secretary of HHS for compliance and investigation purposes, or where it is made pursuant to an authorization. Because business associates are now directly liable under the Privacy Rule, business associates may face stiff penalties for permitting unnecessary access to PHI by staff and for other failures to restrict use, disclosure, and requests for PHI to the minimum necessary. For instance, a law firm must be careful to formulate its requests to its clients for PHI so that only necessary information is produced.

HHS has stated in its commentary accompanying the Omnibus Rule that covered entities and business associates may reasonably rely on the requests of other covered entities and business associates to meet the minimum necessary standard. When it is "reasonable" to rely, of course, is not so easily discerned. Is it reasonable for a law firm to rely upon a subcontractor's records request where, despite the new rules, the subcontractor's request is no more specific than it has been in the past? Surely, closer cases could be stated, but in general, the prudent may decide not to rely on HHS' assurances and tailor their records request forms accordingly.

iii. Business Associate-Subcontractor Agreements

Business associates that contract with subcontractors must also now meet the same requirements as covered entities that contract with business associates. Some of those requirements include:

- Taking reasonable steps to cure a breach or end a violation of the agreement terms, including, if necessary and "feasible," terminating an agreement,
- Including a provision in the agreement that permits such termination,
- Including a provision that requires compliance with the various standards and requirements under the Security and Privacy Rule, and
- Including a provision that calls for the return or destruction of all PHI created or received by the business associate or subcontractor upon termination of the agreement.

45 C.F.R. § 164.504.

iv. Disclosures About Decedents

There is no need to comply with the Privacy Rule when handling the PHI of deceased individuals who have been deceased for more than 50 years. 45 C.F.R. § 164.502. The Omnibus Rule specifically excludes the health information of long dead decedents from the definition of PHI. 45 C.F.R. § 164.103. The easiest way to handle decedents' records may be to destroy them to the extent permitted by state law; however, some records, including a record of disclosures, may need to be maintained.

V. Updated HIPAA Enforcement Rule

The HIPAA Enforcement Rule, 45 C.F.R. Part 160, Subparts C–E, established rules governing the compliance responsibilities of covered entities and business associates with respect to the enforcement process, including the rules governing investigations by HHS; rules governing the process and grounds for establishing the amount of a civil money penalty for HIPAA violations; and rules governing the procedures for hearings and appeals when the covered entity challenges a violation determination. HITECH made several amendments to the Social Security Act to strengthen the HIPAA Enforcement Rule.[1] These strengthening amendments have been incorporated into the Omnibus Rule, and are discussed below.

A. Investigations & Compliance Reviews

HHS enforcement action may consist of (1) a formal complaint investigation and/or (2) a compliance review. Anybody who believes that a covered entity or business associate is not complying with HIPAA may file a complaint. HHS generally conducts compliance reviews to

[1] The Omnibus Rule adds the term ''business associate'' to the following provisions of the Enforcement Rule: 45 C.F.R. §§ 160.300; 160.304; 160.306(a) and (c); 160.308; 160.310; 160.312; 160.316; 160.401; 160.402; 160.404(b); 160.406; 160.408(c) and (d); and 160.410(a) and (c). This is done to implement §§ 13401 and 13404 of the HITECH Act, which impose direct civil money penalty liability on business associates for their violations of certain provisions of the HIPAA Rules.

investigate alleged HIPAA violations that are brought to HHS's attention through mechanisms other than a complaint, such as through a media report or from another state or federal agency.

The Omnibus Rule requires HHS to formally investigate any complaints (and to perform compliance reviews for matters brought to HHS's attention through means other than a complaint) when a preliminary review of the facts indicates a possible HIPAA violation by a covered entity or business associate due to "willful neglect." Willful neglect continues to be defined as the "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." A "preliminary review of the facts" may include additional inquiries beyond just reviewing the allegations of the complaint, as indicated on a case by case basis. HHS also has the discretion to perform complaint investigations or compliance reviews in circumstances not rising to the level of willful neglect.

HHS has the discretion to attempt to resolve noncompliance through voluntary corrective action or other informal means. However, HITECH *requires* HHS to impose civil monetary penalties for any violations due to willful neglect, even if the covered entity or business associate engages in voluntary corrective action.

Covered entities and business associates are required to cooperate with and make information available to HHS during complaint investigations and compliance reviews, including providing requested PHI. HHS is prohibited from disclosing the PHI it obtains except as necessary for determining and enforcing compliance with the Omnibus Rule; for coordinating with other specified law enforcement agencies (such as other agencies enforcing the HIPAA rules, the FTC Act, or the HITECH ACT); or as otherwise required by law.

B. Civil Monetary Penalties; *Mens Rea* Requirement; Factors in Determining Monetary Penalties; Criminal Penalties

HITECH revised section 1176 of the Social Security Act to establish four tiers of penalties to correspond to the levels of culpability and *mens rea* associated with HIPAA violations:

1. Where the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, of a violation (minimum penalty of $100 to $50,000 per violation);

2. Violations due to reasonable cause and not to willful neglect (minimum penalty of $1,000 to $50,000 per violation);

3. Violations due to willful neglect that is corrected within a specified time period (minimum penalty of $10,000 to $50,000 per violation); and

4. Violations due to willful neglect that is not corrected within a specified time period (minimum penalty of $50,000 per violation).

There is no *mens rea* requirement for the first (lowest) category of violation, and the existence of *mens rea* is presumed with respect to the third and fourth categories of violation, as they involve willful neglect. The *mens rea* for the second category of violation is ''reasonable cause,'' which is defined as ''an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.''

All four categories of civil monetary penalties have a maximum penalty of up to $1.5 million for all "identical violations" of an identical requirement or prohibition in a calendar year. However, a separate $1.5 million cap applies for each different requirement or prohibition that is violated in a calendar year. Thus, the total civil monetary penalty could exceed $1.5 million per calendar year by substantial amounts, depending on the number of individuals affected and the number of requirements or prohibitions violated. In addition, these civil monetary penalties are in addition to any other penalties prescribed by law, except that civil money penalties for the same act or omission may not be imposed under both the Omnibus Rule and the Patient Safety Quality Improvement Act (PSQIA).

HHS determines the amount of the "per violation" penalty on a case by case basis, based on enumerated aggravating and mitigating factors, including the nature and extent of the violation; the nature and extent of the resulting harm; whether the violation was beyond the direct control of the covered entity or business associate; the history of prior compliance or noncompliance, including satisfactory corrective action; the size and financial condition of the covered entity or business associate; and other relevant factors. The number of "identical violations'' in a calendar year is determined based on the nature of the covered entity's or business associate's obligations under the provision violated, such as its obligation to act in a certain manner, or within a certain time, or with respect to certain persons.

Continuing violations are penalized as identical violations for each day the violation continues uncorrected. Further, many breaches will involve more than one violation (such as an impermissible use or disclosure, plus a safeguards violation), each of which may lead HHS to impose a separate civil monetary penalty.

HHS has the discretion to waive all or part of the penalties if payment of the penalty would be excessive relative to the violation, or to settle or compromise the amount of a civil monetary penalty. The imposition of a civil monetary penalty may be appealed in a hearing to an administrative law judge.

Under the Omnibus Rule, HIPAA violations remain subject to criminal penalties under the criminal provision of HIPAA (42 U.S.C. 1320d-6). Such criminal violations are prosecuted by the Department of Justice. However, for HIPAA violations occurring on or after February 11, 2011, HHS cannot impose a civil monetary penalty if a criminal penalty has been imposed.

C. Affirmative Defenses

Although HITECH requires the imposition of civil monetary penalties for all HIPAA violations due to willful neglect, covered entities and business associates may establish an

affirmative defense to the imposition of civil monetary penalties under the following circumstances:

1. For violations occurring prior to February 18, 2009, if the covered entity did not have knowledge of the violation, determined in accordance with the federal common law of agency, and, by exercising reasonable diligence, would not have known that the violation occurred;

2. For violations occurring prior to February 18, 2009, if the violation (i) is due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated, (ii) is not due to willful neglect, and (iii) is corrected during either: (a) the 30-dayperiod beginning on the first date the covered entity knew or by the exercise of reasonable diligence would have known that the violation occurred; or (b) such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply;

3. For violations occurring on or after February 18, 2009, if the violation (i) is not due to willful neglect and (ii) is corrected during either: (a) the 30-day period beginning on the first date the covered entity knew or by the exercise of reasonable diligence would have known that the violation occurred; or (b) such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply;

4. Prior to February 18, 2011, if the violation is criminally punishable under 42 U.S.C. § 1320d-6 (regarding wrongful, knowing use or disclosure of PHI); or

5. After February 18, 2011, if criminal penalties have actually been imposed under 42 U.S.C. § 1320d-6.

As is evident from the above, there are no affirmative defenses for violations involving willful neglect, even if the violation is corrected within the 30-day or other period prescribed by HHS.

D. Increased Liability Exposure of Covered Entities & Business Associates for "Agents"

One of the most significant changes to the HIPAA Enforcement Rule is that the Omnibus Rule makes covered entities and business associates liable for the acts *and penalties* of their business associate or subcontractor agents that are committed or incurred while acting within the scope of the agency, determined in accordance with the Federal common law of agency, *regardless of whether the covered entity or business associate has a compliant business associate agreement in place*.

The essential factor in determining whether an agency relationship exists between a covered entity and its business associate (or between a business associate and its subcontractor)

is the right or authority (whether or not exercised) of the covered entity or business associate to control the business associate's or subcontractor's conduct in the course of performing a service on behalf of the covered entity or business associate. The authority of a covered entity or business associate to give interim instructions or directions is the type of control that distinguishes covered entities or business associates in agency relationships from those in non-agency relationships. The commentary to the Omnibus Rule provides that a business associate or subcontractor generally is not an agent if it enters into a business associate agreement with a covered entity or business associate 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 or business associate 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 or subcontractor generally is an agent if it enters into a business associate agreement with a covered entity or business associate that grants the covered entity or business associate the authority to direct the performance of the service provided by its business associate or subcontractor. As in the Federal common law, labeling a business associate or subcontractor as an "independent contractor" does not control whether an agency relationship exists.

Once the determination is made that an agency relationship exists, relevant factors in determining the *scope* of that agency include (1) the time, place, and purpose of the agent's conduct; (2) whether the agent engaged in a course of conduct subject to a covered entity's or business associate's control; (3) whether the agent's conduct is commonly performed by a business associate in service to a covered entity or business associate; and (4) whether or not the covered entity or business associate reasonably expected that the agent would engage in the conduct in question.

VI. Other Considerations for Firms

Law firms who receive protected health information in the course of representing their health care clients qualify as business associates. These law firms may further disclose PHI to persons or entities to assist in those representations and, therefore, create relationships with subcontractors or so-called "downstream business associates." Those relationships are also governed by HIPAA and create potential direct liability for law firms in the event of a HIPAA violation. While each law firm's response to their obligations under HIPAA may differ depending on the nature of the firm, the nature of the relationships, and the particular jurisdiction, the following identifies the questions every law firm should be asking:

A. When are you a Business Associate and which of your subcontractor relationships are governed by HIPAA?

Law firms should inventory their current business associate relationships and recognize when new matters trigger a business associate relationship. Where a business relationship exists, there should be a compliant BAA in place. While BAAs are required to have certain provisions, covered entities may each have their own preferred BAA form, so it is important to ensure each is compliant.

Also, while a law firm may receive PHI from a client as a business associate in one instance, not all representations that require review of an individual's health information from a

covered entity trigger a HIPAA-covered business associate relationship. For example, if medical records are obtained from a covered entity during litigation via a release, a subpoena, court order (or directly from opposing counsel), no business associate relationship has been established. While that information may be considered confidential, the HIPAA privacy, security and breach notification provisions do not apply.

This distinction can be important when assessing which law firm subcontractors are also subject to HIPAA enforcement. For example, a law firm may consult with medical experts, a life care planner, or an economist on a particular matter and provide such consultant with medical records in the course of their review. Whether a HIPAA-regulated subcontractor or downstream business associate relationship has been established depends on how those records were obtained. If the law firm obtained the records as a business associate, a BAA must be executed with the consultant, who must safeguard the information in accordance with HIPAA's requirements. Because of the increased regulatory obligations imposed on business associate and subcontractor relationships, law firms may wish to develop mechanisms either at the attorney or firm level to identify and document how information comes into the firm so appropriate controls over that information can be imposed and documented.

In addition to the specific consultant relationships that may arise in individual representations, depending on how the law firm initially obtained the PHI, some law firm vendors who carry out general functions will also qualify as HIPAA-covered subcontractors. For example, record scanning, copying, storage, or destruction companies and email management service companies may also qualify as downstream business associates of law firms. These relationships need to be identified and appropriate BAAs obtained.

B. Do you have HIPAA policies/procedures and have you done a security assessment?

As business associates, law firms should have policies and procedures with respect to the maintenance, use, and disclosure of PHI and what to do in the event of a breach. This requirement comes not only from the HIPAA regulations but also from the law firm's BAAs with clients. In particular, law firms must conduct a "security assessment" and implement administrative, physical and technical safeguards with respect to any electronic PHI the Firm creates, receives, maintains, or transmits. This includes addressing typical physical security to safeguard the building, offices, files, and computers, including passwords, encryption, and monitoring. Of course, documented training of attorneys and staff on these measures is necessary.

C. Special Technology Considerations

New technologies are changing how law firms prepare cases, conduct expert reviews, and conduct trials. Electronic transmission of information is routine for discussion with clients and consultants. Use of personal electronic devices such as iPads and smart phones, as well as, laptops, cloud storage or file sharing sites, can facilitate and enhance representation of clients in complex medical cases. These new (and old) technologies need to be addressed in the law firm's security plan.

First, encryption should be a priority. While not strictly required by the HIPAA regulations, encryption must be addressed in any security assessment. Furthermore, a breach of encrypted data is not a "breach" under HIPAA requiring notification. Therefore, as a practical matter, encryption of laptops, personal devices, and email transmissions is recommended.

Second, use of cloud storage or file sharing websites creates security concerns, both from the standpoint of HIPAA requirements and attorney-client considerations. Use of such technology, if approved as part of a firm's security assessment, requires entering into a BAA and should be approved by the client.

Third, commentary to the HIPAA Final Rule made clear that safeguards must be in place with respect to "old" technologies, such as photocopiers and faxes because such devices may store copied or transmitted information. Where such information is PHI, those devices must be wiped and/or destroyed in accordance with HIPAA standards.

VII. Conclusion

Prior to the Omnibus Rule, law firms, like other business associates, faced little or no penalties for unauthorized disclosures of PHI. HHS never made the move to audit or penalize law firms for lack of compliance with HIPAA data privacy and security rules, choosing instead to focus regulatory efforts on health care providers and related health care organizations. However, the Omnibus Rule now imposes direct responsibility and penalties upon business associates, including law firms, for unauthorized disclosures.

In order to comply with the new requirements, law firms should evaluate their current business relationships, including those with vendors and subcontractors, and determine which relationships implicate or involve the exchange of PHI. Law firms should develop and implement an appropriate BAA to be executed by vendors and subcontractors that access or retain personal health information, and furthermore should develop a set of standards for determining whether or not to notify an individual regarding breaches of PHI. While it may be tempting for firms to institute a set of standards under which breaches are rarely reported, HHS has made it clear that it expects most, if not all, breaches to be disclosed. It is not yet clear whether HHS will penalize or investigate law firms for minor breaches, but it is clear that law firms would be wise to take efforts to minimize the potential for such breaches, including compliance with the new, and stricter, requirements set forth in the Omnibus Rule.