OMNIBUS RULE IMPLICATIONS FOR COVERED ENTITIES

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 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. 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. Specifically, the following entities are included in the definition of business associates: (1) Health Information Organization, e-prescribing gateway, or other person that provides data transmission services with respect to PHI to a covered entity and that requires routine access to such PHI, (2) a person who offers a personal health record (PHR) to one or more individuals on behalf of a covered entity, and (3) subcontractors that create, receive, maintain, or transmit PHI on behalf of a business associate. Additionally, patient safety activities were added to the list of functions and activities a person may undertake on behalf of a covered entity that give rise to a business associate relationship. 78 Fed. Reg. at 5570-5571.

A. Health Information Organization, E-Prescribing Gateway, or Other Person That Facilitates Data Transmission and Requires "Routine Access" to PHI

The Department of Health and Human Services (HHS) declined to provide a definition for Health Information Organization in the Omnibus Rule recognizing that the industry continues to develop and in turn, the type of entities that may be considered Health Information Organizations continues to evolve. With respect to what it means to require "routine access" to PHI, HHS distinguishes entities that require access to PHI on a "routine basis" from those entities that serve as "mere conduits." 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 the service for the covered entity. HHS cautioned that the "mere conduit" exception is intended to be narrow and exclude only those entities providing mere courier services. "[A] conduit transports 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.

B. Vendors of Personal Health Records

A PHR vendor is a business associate only if they act "on behalf of" a covered entity. A PHR vendor may work on behalf of both the individual directly and a covered entity, but is not a business associate unless it acts on behalf of the covered entity. The mere receipt by a PHR vendor of PHI from a covered entity, such as pursuant to an authorization, does not subject the PHR vendor to HIPAA as a business associate. 78 Fed. Reg. at 5572.

C. Subcontractors

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." The Omnibus Rule provides that "business associate" includes a "subcontractor that creates, receives, maintains, or transmits [PHI] on behalf of the business associate." The analysis of whether a subcontractor is a business associate is the same analysis applied to whether a business associate is acting on behalf of a covered entity. It is 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 on behalf of the business associate. 78 Fed. Reg. at 5572-5574.

D. Examples of Entities Qualifying as Business Associates

- Entity that requires access to PHI in order to perform a service for a covered entity, such as a Health Information Organization that manages the exchange of PHI through a network on behalf of covered entities through the use of record locator services for its participants (and other services). 78 Fed. Reg. at 5572.
- Patient Safety Organizations when engaging in activities such as quality analysis on behalf of covered entities. 78 Fed. Reg. at 5570.
- Data storage company that has access to a covered entity's PHI (whether digital or hard copy) <u>even if</u> the data storage company does not view the PHI or only does so on a random or infrequent basis. 78 Fed. Reg. 5572.
- PHR vendor hired by covered entity to provide and manage a PHR service the covered entity wishes to offer its patients or enrollees, and provides the vendor access to PHI in order to do so. 78 Fed. Reg. at 5572.
- PHR vendor that operates a PHR on behalf of a covered entity and has access to PHI, even if the PHR vendor does not exercise that access. 78 Fed. Reg. at 5572.
- Company hired by business associate to handle document and media shredding for the secure disposal of paper and e-PHI. 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.

E. Examples of Entities Not Qualifying as Business Associates

- 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 associate's own management, administration or legal responsibilities and not related to the business associate's responsibilities to the covered entity. 78 Fed. Reg. at 5573.

F. Business Associate Agreements

Section 164.504(e) sets forth in detail the specific requirements for business associate agreements (BAAs). Sample provisions for a BAA have been published on HHS' website at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html. 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 BAAs with the subcontractors of its business associates. A covered entity's business associate must execute and have in place BAAs with its subcontractors. Although business associates are required by law to have a BAA with their subcontractors, covered entities may want to consider including this requirement in their BAA. A covered entity is not in compliance with the Omnibus Rule "if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible." 45 C.F.R. 164.504(e). As will be discussed in Section V below, the Omnibus Rule provides for increased penalties for noncompliance and potential liability for covered entities based on the acts/omissions of their business associates under an agency theory. *See* 45 C.F.R. 160.402(c). Thus, there will likely be more consideration given to provisions in BAAs that address indemnification.

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 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 notification. Covered entities and business associates must now overcome a presumption that any breach requires notification and <u>must</u> 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. Before, only covered entities were obligated to comply with these Rules. 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.

While we expect many of our readers to be covered entities and, as a result, question the relevance of this section to their own privacy strategies, it is important for covered entities to be aware of their business associates' obligations. As discussed under the Business Associate Agreements section above, covered entities can incur liability if they do not respond appropriately to their business associates' failures to fulfill these obligations.

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, as the name implies, are very general and act more like conceptual guidelines for handling electronic protected health information ("ePHI"). The standards are more specific than the general requirements and outline the parameters of the Security Rule, but are still quite general. The implementation specifications are the instructions for implementing the standards. Therefore, the implementation specifications will be the most specific and useful to achieving compliance. All parts of the Rule, however, must be considered to achieve a level of understanding necessary to evaluate existing practices and implement new ones.

While much of this information is not new, it may be new to many business associates, so it is explored below. A bit of warning (or reassurance, depending on how you look at it): none of these concepts is explored comprehensively or with the level of detail needed to achieve compliance. This should, however, 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 covered entities and now business associates must ensure the confidentiality, integrity, and availability of all 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.

Business associates, just like covered entities, are permitted some flexibility in designing practices and policies to comply with the Security Rule. The covered entity or business associate may use any security measures that reasonably and appropriately achieve the requirements of the Security Rule. To be reasonable and appropriate, the measures must take into account the probability and severity of risk to ePHI. The cost and size and technical capabilities of the entity are also relevant. The reasoning behind this rule should be obvious. A prison cannot be expected to use the same procedures as a hospital and a small medical provider cannot be expected to institute an IT strategy as elaborate or sophisticated as that of a giant health plan.

ii. The Standards

There are different categories of standards, including administrative safeguards, physical safeguards, technical safeguards, organizational requirements, and policies and procedures and documentation requirements. Each category of standard has its own implementation specifications that may be either required or addressable. Addressable implementation specifications are still required, but permit alternative measures if they achieve the purposes of the specification. Favoring simplicity, we decline to distinguish between standards and the two types of implementation specifications.

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.

> 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 as 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. Covered entities and 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 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 workstations.
>
> Standard 3: Physically safeguard workstations that access ePHI.
>
> Standard 4: Control the handling of electronic media, including computers and their hard drives if they contain ePHI. 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 the 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. Your *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. Unlike the Security Rule, which applies nearly identically to covered entities and business associates, the Privacy Rule makes some distinctions, mostly concerning the business associate agreement. 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.

i. Required and Permissible Disclosures

The instances when disclosures of PHI by business associates are required or permissible generally include the same instances when such disclosures would be required or permissible for covered entities. As promised, however, there are a few important distinctions. Business associates must disclose PHI where it is required by their agreement *or* by law and they may only disclose PHI where it is permitted both by law *and* by the business associate agreement. In case it isn't obvious, this is a distinction because covered entities, generally speaking, are not subject to business associate agreements.

An additional exception permits business associates to disclose PHI for their own proper management and administration or to permit the business associate to provide data aggregation services to a covered entity. Business associates are also required to disclose PHI to the covered entity to satisfy a request by the individual that PHI be produced in an electronic format.

ii. Getting Assurances From Subcontractors

The Privacy Rule requires that covered entities get assurances from business associates that they will adequately protect PHI before disclosing such information. 45 C.F.R. § 164.308. Because the Omnibus Rule treats subcontractors who deal with PHI on behalf of business associates as also being business associates, covered entities could have been saddled with the further onerous obligation of seeking assurances from the subcontractors of business associates. The Omnibus Rule relieves covered entities of this obligation by stating that covered entities do not need to obtain such assurances from subcontractors. To cover this gap in protection, however, business associates are obligated to obtain assurances from their subcontractors that they will adequately protect PHI. As before, all assurances must be documented in written business associate agreements.

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.

C. Disclosures About Decedents

There are several provisions addressing disclosures of decedents' PHI. Some are nothing new, such as the exceptions for disclosures for research purposes, to law enforcement if criminal activity is a suspected cause of death, or to coroners and funeral directors as necessary to carry out their duties.

One new noteworthy provision requires covered entities to comply with the Privacy Rule when handling the PHI of deceased individuals until they have been deceased for more than 50 years. 45 C.F.R. § 164.502. The wisdom behind this particular time period is debatable, but HHS expressed little concern for the burden of this provision because allegedly there was scant information about whether reducing the time period would provide a cost-savings to covered entities and business associates. The easiest way to handle decedent's 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.

Covered entities may disclose PHI to family members of decedents under the new Rules. 45 C.F.R. § 164.510. Provided such disclosure is consistent with the decedent's known preferences, covered entities may disclose PHI to family members or other persons who paid for care or who were involved in care. To be clear, covered entities and business associates are not required to make such disclosures; it is entirely optional.

This exception limits disclosure of information relevant to that person's prior involvement in the decedent's care. The comments accompanying the Omnibus Rule seem to play loose with this requirement, however, by suggesting that a covered entity could disclose the circumstances of death to a family member who did not necessarily have any involvement in care. Certainly, however, a third-party should not be given access to a decedent's PHI simply because he or she elected to pay the decedent's medical bills.

An interesting but arguably less important twist is that the Omnibus Rule also specifically excludes the health information of long dead decedents from the definition of PHI. 45 C.F.R. §164.103. Therefore, this information is unprotected under HIPAA/HITECH and may even be sold or commercially exploited. The discussion accompanying the Omnibus Rule even acknowledges this possibility.

D. Disclosure of Student Immunization Records

The Omnibus Rule includes a new exception from the written authorization requirement for student immunization records. 45 C.F.R. § 164.512(b)(1). A covered entity may disclose PHI to a school at which the individual in question is a student or prospective student if:

- The PHI is limited to proof of immunization,
- State or other law requires such information to grant admission to the school, and
- The covered entity obtains and documents the agreement of a parent, guardian, or other person acting in loco parentis (if the student is an emancipated minor or adult, only that student's agreement will suffice).

To meet the documentation requirement, documentation should be reasonable in light of the mode of agreement. The following methods should all be sufficient:

- A concise written description of the phone call, if assent is obtained by phone
- Saving a copy of the email, if assent is obtained by email
- A concise written description of the discussion, if assent is obtained in person, or
- Saving a copy of the letter, if assent is obtained by letter.

Covered entities cannot rely upon opt-out agreements or notices. Opt-out agreements or notices are those where permission is presumed unless the parent, guardian, or individual objects. These are insufficient and will constitute a violation of HIPAA/HITECH. Valid agreements, however, are valid until the permission is revoked by the person with authority to do so (parents, guardians, or the adult or emancipated student).

To the extent there are concerns about whether the Family Educational Rights and Privacy Act ("FERPA") interacts with this provision, generally it does not unless the organization is a hybrid entity that contains both a component subject to the requirements of HIPAA/HITECH and a component that receives funds under a program administered by the U.S. Secretary of Education. For such organizations, the question of complying with both laws is broader than just what to do about immunization records and the advice of counsel should be sought.

E. Access to PHI Maintained Electronically

As discussed above, there are many requirements, standards, and implementation specifications that covered entities, business associates, and even their subcontractors must follow regarding the protection of ePHI. Any device containing ePHI must be protected by multiple layers of physical, software-based, and administrative safeguards and controls. What about when an individual wants access to his or her PHI in electronic form?

Under the Omnibus Rule, individuals have the right to demand access to their ePHI in any electronic form. 45 C.F.R. § 164.524. If the requested form is not feasible, then the covered entity may supply the information in any readable electronic form. Covered entities must also send the information to third parties designated by the individual to receive the information, but only if a signed, written authorization that indicates the intended recipient and where the information should be sent is provided to the covered entity. Generally, covered entities will have thirty days to comply with such requests. The comments to the Omnibus Rule indicate that HHS regards this mandate as requiring covered entities with older systems, which may not be able to provide electronic copies, to invest in the technology sufficient to provide some form of electronic copy of health records.

Of course, a covered entity is not required to provide PHI in every case. The Omnibus Rule lists many specific and limited situations in which access may be denied. Depending on the basis for the denial, the covered entity may, however, be obligated to supply an appeal process, called a review. The covered entity must designate a licensed healthcare professional who did not take part in the initial decision to act as the reviewing official. Some reviewable and non-reviewable denials of requests include:

Reviewable

- Denials to protect the physical safety of the individual or another person,
- Denials of requests for information that reference another person and where disclosure would risk substantial harm to the other person, and
- Denials of requests for information by a personal representative where disclosure would risk substantial harm to the individual or another person

Non-Reviewable

- Denials of requests for psychotherapy notes,
- Denials of requests for information compiled in reasonable anticipation of use in a legal proceeding or action, and
- Denials of requests for information obtained or created by a provider in the course of research, provided that the individual agreed to the denial and that the individual is informed that his or her access will be restored upon completion of the research.

45 C.F.R. § 164.524.

F. Recouping Costs

While the costs of complying with HIPAA/HITECH will be born in large part by the covered entities and their business associates, such entities are permitted to recover some of the costs of producing PHI. When production of PHI is requested, the covered entity is permitted to charge a reasonable, cost-based fee. 45 C.F.R. § 164.524. What is reasonable and cost based, however, is specifically limited. A reasonable, cost-based fee may include:

- The cost of labor for copying,
- The cost of labor for making e-copies,
- The cost of labor to compile, extract, scan, and burn PHI to electronic format for the purpose of complying with a demand,
- The cost of postage, if mailing is requested, and
- The cost of supplies to make copies, including paper, a CD, or flash drive, if requested,

but not:

- The cost of acquiring new technology to provide PHI in the electronic format requested,
- The cost of maintaining data systems,
- The capital cost of access and storage infrastructure, or
- The labor cost of paper or data retrieval.

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 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.

---

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.

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 increasing penalty amounts 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, 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-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;

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. Conclusion

Prior to the Omnibus Rule, business associates faced little or no penalties for unauthorized disclosures of patient information. However, the Omnibus Rule now places direct responsibility, and penalties, upon business associates for unauthorized disclosures. Covered entities and business associates should both assess which of their vendors are now business associates or subcontractors under the Omnibus Rule. To the extent an existing vendor is now characterized as a business associate or subcontractor under the Omnibus Rule, a business associate agreement will need to be put in place before September 23, 2013. Furthermore, all business associate agreements, new or old, should be drafted or revised to ensure compliance with the Omnibus Rule. Likewise, given the new presumption of reportable breach, covered entities and business associates should both revise, or in the case of business associates, develop breach notification policies and response plans.

Now that business associates are directly bound by rules governing permissible uses of PHI, breach notifications, and cooperation with HHS in investigations, business associates should develop their own separate policies and procedures for compliance with the Omnibus Rule. Employees who use or transmit PHI in the normal course of their duties should be made aware of such policies and procedures and be expected to comply with the same. Of note, covered entities are responsible for monitoring compliance with their business associates. As such, covered entities should take steps to ensure that their business associates have instituted appropriate policies and procedures and monitor compliance on an ongoing basis.