Jan 30 2013

Practice Area: Health Law & Health Information Privacy and Security

On January 17, 2013, the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") released the long awaited omnibus final rule entitled *Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules* (the "Omnibus Rule"). The Omnibus Rule consists of four final rules that:

1. Finalize modifications to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy, Security, and Enforcement Rules to implement the Health Information Technology for Economic and Clinical Health ("HITECH") Act;
2. Adopt changes to the HIPAA Enforcement Rule to incorporate the HITECH Act's increased and tiered civil money penalty structure;
3. Modify the Breach Notification Rule; and
4. Finalize modifications to the Privacy Rule to incorporate requirements of the Genetic Information Nondiscrimination Act of 2008 ("GINA").

The four rules that make up the Omnibus Rule enhance and create consumer privacy protections; expand requirements for and liability of business associates; bolster OCR's investigative and enforcement authority; and strengthen and modify breach notification requirements. The Omnibus Rule will require a significant investment of time and resources for covered entities and business associates to ensure compliance.

The Omnibus Rule will be effective on March 26, 2013, and covered entities and business associates must comply with a majority of the provisions by September 23, 2013. However, the 180-day compliance period does not apply to (i) modifications to the Enforcement Rule, which are effective in March 2013 with the Omnibus Rule or as otherwise specified, or (ii) certain provisions for which HHS has defined a different compliance period (e.g., business associate agreements discussed below).

This *Update* outlines provisions of the Omnibus Rule that are significant for health care providers, health plans, and business associates, and provides recommendations for implementation of and compliance with the new requirements.

I. Consumer Protections and HITECH Requirements

Beyond the requirements of the HITECH ACT, the Omnibus Rule expands existing consumer rights and introduces new consumer rights. Significant consumer protection provisions include the following:

Marketing
Covered entities and business associates must meet new requirements when using protected health information ("PHI") to market a product or service to patients. The Omnibus Rule generally defines "marketing" as "any communication about a product or service that encourages recipients of the communication to purchase or use the product or service." However, there are exceptions for certain health-related communications (discussed below).

Entities must obtain prior written authorization before: (i) sending marketing communications to patients where the covered entity receives direct or indirect financial remuneration from a third party whose product or service is being marketed in exchange for making the communication; or (ii) giving or selling patient PHI to a third party for marketing purposes.

"Financial remuneration" means a direct or indirect payment from or on behalf of a third party to the covered entity (or business associate of the covered entity) in exchange for making a communication which encourages the recipient to use or purchase a product or service offered by the third party. For purposes of the marketing authorization requirement, financial remuneration does not include non-financial or in-kind benefits provided by a third party.

HHS provides examples in the Omnibus Rule preamble in clarifying what is marketing for purposes of the authorization requirement:

- Prior authorization is required prior to communications to patients regarding the acquisition of new state-of-the-art medical equipment if the equipment manufacturer paid the covered entity to send the communication to the patients.
- Prior authorization is not required prior to communications to patients regarding the acquisition of new state-of-the-art medical equipment if a local charitable organization, such as a breast cancer foundation, funded the communication to the patients.
- It would not constitute marketing and no authorization is required if a hospital mailed flyers to its patients announcing the opening of a new wing where the funds for the new wing were donated by a third party. No authorization is required in this situation because the financial remuneration to the hospital was not in exchange for mailing the flyers.

Exceptions to the marketing authorization requirement include: face-to-face communications, communications that do not promote a product or service from a particular provider, communications about government and government-sponsored programs (*e.g.*, BadgerCare, Medicare), refill reminders, and communications about a drug or biologic currently prescribed to the patient.

There is a limited exception for financial remuneration received in exchange for providing a refill reminder or communicating about a drug or biologic currently prescribed to the individual. An entity may receive a "reasonable amount" of remuneration for providing these types of communication without authorization. A "reasonable amount" includes only labor costs, supplies, and postage to make the communication. If the third-party payment generates a profit or includes payment for other costs, it is not a "reasonable amount" under this exception and therefore authorization would be required.

In addition to the elements of a valid HIPAA authorization, marketing authorizations must also disclose that the covered entity is receiving financial remuneration and must adequately describe the intended purpose (or scope) of the requested uses and disclosures. The authorization form must clearly state that the patient may revoke the authorization at any time.

Fundraising
The Omnibus Rule makes minor changes to fundraising requirements under HIPAA. Types of communications that are considered "fundraising" are not changed, but the Omnibus Rule expands the PHI available to fundraisers and also strengthens individuals' ability to opt out of receiving fundraising materials.

All fundraising communications must include a clear and conspicuous mechanism for the recipient to opt out of receiving future communications. The mechanism for opting out must not be unduly burdensome or costly for the individual. For example, covered entities may use a toll-free number, email address, or other similarly quick and inexpensive option. In the preamble discussion, HHS notes that it is still assessing whether a requirement for an individual to write and send in an opt-out letter would be unduly burdensome.

Entities have discretion regarding the scope of the opt-out options provided to individuals. For example, the entity could offer that the recipient may opt out of all future fundraising communications or that the recipient may opt out of fundraising communications regarding specific campaigns. However, in either case, if an individual has opted out of receiving fundraising communications, this is to be treated as a revocation of authorization to use or disclose PHI for this purpose.

Right to Electronic Copy of Electronic Medical Record
The Omnibus Rule outlines a new consumer right to an electronic copy of the patient's medical record. Covered entities must provide an individual with access to the individual's PHI in electronic form, if: (i) the individual requests to view or receive an electronic copy of PHI; and (ii) the entity maintains PHI electronically in one or more designated record sets.[1] To the extent possible, the entity is to provide access in the format requested by the individual. The entity is not, however, required to purchase a full scope of new software to accommodate requests of this nature.

In fulfilling this requirement, covered entities are permitted to send individuals unencrypted emails if the individuals prefer such format after advising individuals of the risk of such format. Covered entities are not responsible for unauthorized access of PHI while in transmission to the individual based on the individual's request. Further, the individual may direct the covered entity to transmit a copy directly to the individual's designee, provided that the individual does so in a clear, conspicuous, and specific manner.

Right to Restrict Disclosures to Health Plans
The Omnibus Rule outlines a new consumer right to restrict disclosures of PHI to health plans in certain circumstances. An individual may restrict the disclosure of PHI to a health plan (or the health plan's business associate) if:

- The disclosure is for payment or health care operations;
- The disclosure is not otherwise required by law; and
- The individual has paid the covered entity in full for the item or service.

Providers should develop methods of flagging records so that restricted PHI is not available to the health plan. Providers should also be prepared to develop new operational policies for these "paid in cash" restrictions in order to address bundled services and health maintenance organization ("HMO") prohibitions on accepting payment above individual cost sharing amounts. A provider may need to counsel patients on the provider's ability (or inability) to unbundle claims and that the patient may need to seek out-of-network care in order to restrict disclosure of PHI to an HMO. Providers should review and update payer contracts because contractual requirements to submit claims or disclose PHI do not exempt providers from this obligation.

Notice of Privacy Practices
The Omnibus Rule modifies what statements are required in a provider and health plan Notice of Privacy Practices ("NPP") and loosens distribution requirements for health plans. The NPP must contain statements indicating, as applicable:

- That most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require the individual's authorization;
- That other uses and disclosures not described in the NPP will be made only with the individual's authorization;
- That the entity may use PHI for fundraising and the individual has a right to opt out of such a use;
- The individual's right to restrict disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service;
- A health plan's statement that it is prohibited from using PHI that is genetic information for underwriting purposes (discussed below); and
- The individual's right to be notified following a breach of unsecured PHI.

Health care providers with direct treatment relationships with an individual are not required to change NPP distribution requirements under the Omnibus Rule. However, the revised NPP must be posted in a prominent location and available to an individual upon request.

Health plans that currently post NPPs on their websites must (i) post the material change or revised NPP on its website by September 23, 2013; and (ii) provide the revised NPP, or information about the material change and how to obtain the revised NPP, in the health plan's next annual mailing.

Health plans that do not have customer service websites must provide the revised NPP, or information about the material change and how to obtain the revised NPP, to covered members within 60 days of the revision to the NPP.

Genetic Information Requirements
As required by GINA, HHS amended the Privacy Rule to prohibit health plans, health insurance issuers, and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes. The Omnibus Rule applies this prohibition to all health plans that are covered entities under HIPAA, with the exception of issuers of long-term care policies. The prohibition is applied to all genetic information from the compliance date of the Omnibus Rule, regardless of where the genetic information originated.

The definition of "health information" has been updated to include genetic information. Consequently, genetic information is now a specific type of health information that is protected under HIPAA. In defining "genetic information," HHS clarified that information concerning the manifestation of a disease or condition in a family member constitutes genetic information about an individual, but information concerning the manifestation of a disease or condition in the individual does not constitute genetic information about the individual. As a result, information concerning the manifestation of a disease or condition in an individual may be used by health plans for underwriting purposes.

The Omnibus Rule does not incorporate GINA requirements as a complete prohibition on the use and disclosure of genetic information. There are circumstances under which a health plan may appropriately obtain and use genetic information (*e.g.*, for payment purposes). The health plan may not, however, use or disclose genetic information for purposes of underwriting. A violation of the use of genetic information may subject a health plan to penalties for violation of both existing nondiscrimination restrictions and new privacy protections under the Omnibus Rule.

The Omnibus Rule also requires health plans to update NPPs to include a statement that they are prohibited from using or disclosing genetic information for underwriting purposes. To comply with the new GINA provisions, health plans will need to review their policies and procedures relating to the use of genetic information and update their NPPs, if they have not already been changed to reflect the statutory changes.

II. Business Associates

The Omnibus Rule includes significant changes and consequences for business associates and subcontractors of business associates.

Defining "Business Associate"
The Omnibus Rule expands the definition of a "business associate" to include persons or entities, other than members of the covered entity's workforce, that create, receive, maintain, or transmit PHI on behalf of a covered entity. The definition of "business associate" was also revised to expressly include subcontractors of business associates.

Under the expanded definition, "business associate" includes:

- A 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 access on a routine basis to such PHI;
- A person that offers a personal health record to one or more individuals on behalf of a covered entity; and
- A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate. Subcontractors do not include third parties that receive PHI from a business associate solely for the management, administration, or legal responsibilities of the business associate.

The expanded definition provides a clearer picture of the vendors and entities that fall within the definition. The addition of the word "maintains" to the definition of a business associate expressly includes physical and electronic (*e.g.*, cloud) storage facilities within the definition of a business associate.

The definition of "business associate" does not include:

- A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of an individual;
- A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor;
- A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law; and
- A covered entity participating in an organized health care arrangement that performs a function, service, or activity on behalf of such organized health care arrangement.

Adapting to current technology, entities that transmit PHI are now business associates even if they do not access or view the PHI. Only entities that act as "mere conduits" for transporting PHI but do not access the PHI "other than on a random or infrequent basis" are exempted from the definition of a business associate, such as the U.S. Postal Service. This conduit exception does allow an entity to temporarily store transmitted data incident to transmission without being deemed a business associate.

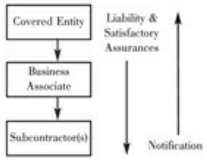
The Omnibus Rule establishes that a person or organization becomes a business associate by definition, not by the act of contracting with a covered entity or otherwise. In other words, any person or organization who performs functions or activities on behalf of, or certain services for, a covered entity or another business associate that involve the use or disclosure of PHI is, by definition, a business associate and is therefore liable for any impermissible uses and disclosures—whether or not that person or entity has entered into a Business Associate Agreement ("BA Agreement").

Permitted Uses and Disclosures
The Omnibus Rule provides that business associates are permitted to use or disclose PHI only as permitted or required by BA Agreements or as required by law. Further, with the exception of uses or disclosures for the business associate's proper management and administration, business associates are expressly prohibited from using PHI in a manner that would violate the Privacy Rule if done by the covered entity.

The expanded business associate requirements under the Omnibus Rule require that business associates comply with the minimum necessary standard for uses and disclosures of PHI, including requests for PHI from another covered entity or business associate. HHS contemplates that the application of the minimum necessary standard may vary between business associates. A business associate must be required to limit uses and disclosures of PHI consistent with the covered entity's policies and procedures, but the BA Agreement should document any additional specific requirements to meet this requirement.

Direct Liability
The Omnibus Rule clarifies the increased liability of business associates and their subcontractors. OCR has direct enforcement authority over business associates and subcontractors. Prior to the Omnibus Rule, business associate liability was limited to failure to comply with BA Agreement terms, and subcontractors were not required to comply with HITECH. The Omnibus Rule expands liability for HIPAA civil and criminal penalties to business associates and subcontractors.

Business associates and subcontractors must comply with the technical, administrative, and physical safeguard requirements in the Security Rule and the use and disclosure requirements in the Privacy Rule. Business associate liability now flows down to all subcontractors (not just the first level of subcontractors), as the Omnibus Rule extends compliance requirements to all subcontractors that handle PHI on behalf of covered entities.



In order to comply with expanded liability, business associates must obtain satisfactory assurances required by the HIPAA Privacy and Security Rules from subcontractors. Such assurances must be documented in an agreement between the business associate and subcontractor (a downstream BA Agreement). Downstream BA Agreements must require subcontractors to notify the business associate of any security incidents or breaches. Once notified by its subcontractor, a business associate must notify the covered entity pursuant to the satisfactory assurances outlined in the BA Agreement with the covered entity.

Business associates must also comply with the requirements of the Privacy Rule applicable to the covered entity to the extent the business associate carries out the covered entity's obligations under the Privacy Rule.

Expanded business associate liability may affect covered entities as well as business associates. If a covered entity knows of a pattern or practice of a business associate that constitutes a breach or violation of HIPAA or the BA Agreement, the covered entity has an obligation to take reasonable steps to cure the breach, end the violation, or terminate the contract. In addition, covered entities are liable for violations resulting from the acts or omissions of business associates that are agents of the covered entity acting within the scope of agency. Likewise, business associates are liable for violations resulting from the acts or omissions of subcontractors that are agents of the business associate acting within the scope of agency.

BUSINESS ASSOCIATE LIABILITY

Business associates are directly liable for compliance with certain Privacy and Security Rule requirements, including:

- Impermissible uses and disclosures of PHI that are not in accord with BA Agreement or the Privacy Rule;
- Failure to provide breach notification to the covered entity;
- Failure to make reasonable efforts meet the minimum necessary standard;
- Failure to provide an accounting of disclosures;
- Failure to enter into BA Agreements with subcontractors that create or receive PHI on the business associate's behalf;
- Failure to disclose PHI when required by the Secretary of HHS to investigate or determine the business associate's compliance with HIPAA;
- Failure to disclose, consistent with the terms of the BA Agreement, PHI to the

covered entity, individual, or individual's designee in order to satisfy a covered entity's obligations regarding an individual's request for an electronic copy of PHI; and
- Failure to comply with the Security Rule.

In addition to direct liability, a business associate is also contractually liable for requirements set forth in the BA Agreement.

OCR will apply the federal common law of agency to determine whether a downstream entity

(business associate or subcontractor) is the agent of the upstream entity (covered entity or business associate). The analysis is based upon the BA agreement and the facts and circumstances of the relationship.

Tips for Compliance
Covered entities should modify existing BA Agreements and enter into additional agreements with newly defined business associates. In addition, business associates must now enter into agreements with subcontractors that include applicable Privacy and Security Rule provisions.

This expanded liability may present practical issues for business associates who work with subcontractors that express an inability or unwillingness to comply with HIPAA. Such a situation will require an evaluation of the business associate's ability to fully comply with HIPAA and the terms of its BA Agreement with the covered entity. The business associate must make a business decision that fully considers the consequences of the subcontractor's shortcomings related to information privacy and security.

Terms of updated and new BA Agreements will be crucial:

- Agreements should clearly specify authorized uses and disclosures because business associates and subcontractors may only disclose PHI as permitted by the BA Agreement, the underlying agreement, or as required by law.
- Agreements should outline compliance with minimum necessary standard.
- Each agreement in the business associate chain must be at least as stringent as the above agreement in the chain, because subcontractor agreements may not permit uses or disclosures that are not permissible if done by the business associate.

Existing BA Agreements must be updated and compliant with Omnibus Rule provisions by September 22, 2014. Covered entities should aim to have updated BA Agreements in place with enough time for business associates to secure agreements with their subcontractors prior to the compliance date, September 22, 2013. Covered entities and subcontractors should work with legal counsel to update existing and draft new BA Agreements for compliance with Omnibus Rule provisions.

III. Stepped Up Investigation, Enforcement, and Civil Money Penalties

The Omnibus Rule expands OCR's ability and obligation to investigate alleged HIPAA violations and enforce HIPAA requirements directly against business associates.

Investigations and Enforcement
OCR must formally investigate *any* complaint if a preliminary investigation of the facts indicates a *possible* violation due to willful neglect. Further, OCR has discretion to conduct a compliance review or complaint investigation of covered entities and business associates when a preliminary review indicates a degree of culpability less than willful neglect. According to the preamble to the Omnibus Rule, these modifications were added to OCR's enforcement authority in order to ensure consistent investigations regardless of whether investigations were initiated by a complaint or compliance review.

The Omnibus Rule allows OCR to resolve investigations or compliance reviews by informal means. However, OCR is permitted to move directly to a formal process, including the issuance of a civil money penalty ("CMP" or "penalty"), without first exhausting informal resolution efforts.

Imposition of Penalties
HITECH established four tiers of increasing penalty amounts that correspond to levels of culpability associated with the violation, and the Omnibus Rule finalizes the penalty structure:

Violation Category	CMP for Each Violation	Violations of an Identical Provision in a Calendar Year
Entity did not know and by exercising reasonable diligence, would not have known that it violated the applicable provision	$100 to $50,000	$1,500,000
Violation due to reasonable cause and not willful neglect	$1,000 to $50,000	$1,500,000
Violation due to willful neglect and was corrected during 30-day cure period beginning on the first day the entity knew or by exercising reasonable diligence, would have known that the violation occurred	$10,000 to $50,000	$1,500,000
Violation due to willful neglect and was not corrected during 30-day cure period	$50,000	$1,500,000

The Omnibus Rule clarifies the definition of a "reasonable cause" violation with regard to the other penalty tiers. "Reasonable cause" means 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.

With all violation categories, penalty amounts will be determined on a case-by-case basis depending on five factors: (i) nature and extent of the violation; (ii) nature and extent of the harm resulting from the violation; (iii) history of prior compliance and noncompliance; (iv) financial condition of the entity; and (v) such other matters as justice may require.

The preamble provides guidance on the methodology by which OCR will count violations for purposes of determining the appropriate CMP. First, identical violations of the permissible use and disclosure standard will be counted by the number of individuals affected. Second, identical violations of the safeguard standard will be counted on a per-day basis (*i.e.*, number of days entity did not have appropriate safeguards in place). Further, OCR may levy a separate penalty for violations which include an impermissible use or disclosure, as well as a violation of the safeguard provisions.

With regard to the maximum CMP that may be assessed against an entity in a calendar year, OCR may calculate a violation of each requirement separately. Consequently, one entity may be subject to multiple penalties of up to $1.5 million annually for violations in each violation category. Consequently, aggregate penalties may total above $1.5 million annually.

OCR is required to impose a penalty for violations due to willful neglect. In addition, the 30 day cure period for violations due to willful neglect (like violations due to all other levels of culpability) begins on the date that the entity first acquires actual or constructive knowledge of the violation. Internal indications of potential noncompliance, including "unusual access or audit log activity" could establish the requisite knowledge. Further, in certain circumstances, a business associate's constructive knowledge may be imputed to the covered entity even if a business associate fails to notify the covered entity. Entities will have the opportunity to submit evidence demonstrating its level of knowledge or lack of knowledge during an OCR investigation; however, demonstrating a lack of actual or constructive knowledge may be a difficult feat for entities.

Penalties for Business Associates
Business associates also face CMP liability under the Omnibus Rule penalty structure. A business associate may be liable for penalties for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, regardless of whether a compliant BA Agreement is in place. Business associate and subcontractor liability is based on the federal common law of agency, and the analysis is fact-based, taking into account the terms of the BA Agreement as the ongoing relationship of the party, including whether the covered entity has the right or authority to control the business associate's conduct.

OCR will have increased flexibility in determining the entities subject to investigation and penalties as well as the methodology by which violations are calculated and assessed. This increased flexibility, in conjunction with the expansion of mandatory investigations and express permission for OCR to impose penalties without first exhausting administrative remedies, indicates that OCR intends to ramp up its investigations and enforcement. Covered entities and business associates should be prepared to present documentation regarding efforts to maintain an active and robust compliance program and appropriate organizational responses to HIPAA violations.

IV. Breach Notification Rule

The Omnibus Rule made two significant changes to the HITECH Breach Notification Rule. First, HHS flipped the presumption as to when notification of a breach is required. An impermissible use or disclosure of PHI is presumed to be a breach, and notification is required, unless an entity can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment.

Second, the risk of harm standard has been replaced with a specific risk assessment standard to determine if there is a low probability that the PHI has been compromised. The risk assessment includes four elements:

1. The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification;
2. The unauthorized person who 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 to the PHI has been mitigated.

If the risk assessment fails to demonstrate that there is a low probability that PHI has been compromised, the entity must provide notification of the breach.

Consistent with the language of the HITECH Act, a breach shall be treated as "discovered" by a covered entity on the first day the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity. In addition, violations of the minimum necessary standard are not exempt from breach notification obligations. Finally, because every breach of unsecured PHI must have an underlying impermissible use or disclosure, OCR has the authority to impose a penalty for the underlying Privacy Rule violation, even in cases where all breach notifications were provided in compliance with HIPAA.

Covered entities and business associates should review breach investigation and notification policies to ensure that all of the required risk assessment factors are included. Although it is not yet known whether the new presumption and risk assessment standard will lead to different results, entities should consider using both the risk of harm and risk assessment standard for investigations of all impermissible uses or disclosures. This practice will allow entities to get comfortable with the risk assessment prior to the September, 2013 compliance date for the standard.

V. Additional Provisions of the Omnibus Rule

In addition to the provisions outlined above, the Omnibus Rule also adds and modifies the following requirements:

- *Sale of PHI*. Covered entities and business associates are generally prohibited from selling PHI without an authorization from the individual. "Sale of PHI" is defined as a disclosure of PHI where the covered entity or business associate receives remuneration (direct or indirect) from or on behalf of the recipient of the PHI in exchange for the PHI. A "sale of PHI" does not include exchange of PHI through a Health Information Exchange.

- *Research Authorizations*. The Omnibus Rule permits use of compound authorizations for research activities, which means that the authorization for the use or disclosure of PHI may be combined with another type of written authorization for the same or another research study (*e.g.*, signed consent to participate in the research study). Where the health care provider conditions the provision of treatment payment, health plan enrollment, or eligibility for benefit on the patient's authorization to use or disclose PHI, the compound authorizations must clearly distinguish between the conditioned and unconditioned research components. Such research authorizations must include the core elements of a HIPAA authorization, and individuals must affirmatively authorize unconditioned research activities.

  It is permissible to obtain authorization for the use and disclosure of PHI for future research if the authorization adequately describes this future use or disclosure. These modifications provide researchers and IRBs with increased flexibility.

- *Decedent PHI*. The Privacy Rule limits the period for protection for a decedent's PHI to 50 years following the individual's death. Family members and others involved in the care of the decedent will have greater access to the decedent's PHI.

- *Student Immunizations*. Requirements for providers to release student immunization records to schools were eased. A covered entity may disclose proof of immunization to a school where state or other law requires the school to have such immunization information prior to admitting the student. Covered entities are permitted to disclose this information upon oral authorization from a parent, guardian or other person acting *in loco parentis* for the student or directly from an adult student or emancipated minor student. Under current Wisconsin law, providers are required to report the vaccination of students without authorization of parents; therefore, this does not alter the requirements for Wisconsin health care providers.

- *Hybrid Entities*. The health care component of a HIPAA Hybrid Entity must include all business associate functions of the entity within the health care component. With respect to a hybrid entity, the covered entity itself—not merely the health care component—remains responsible for complying with regulations regarding business associates and other organizational requirements. Hybrid entities may need to execute legal contracts and conduct organizational matters at the level of the legal entity rather than at the level of the health care component.

VI. Next Steps for Compliance

HHS estimates that the aggregate cost of compliance for the Omnibus Rule's provisions will amount to between $114 million and $225.4 million in the first year of implementation with subsequent years requiring approximately $14.5 million annually. Covered entities, business associates, and subcontractors will all incur costs in coming into compliance with the full scope of the Omnibus Rule's requirements. Entities should assess legal requirements, financial considerations, and operational realities in order to prioritize next steps for compliance.

COMPLIANCE CHECKLIST FOR COVERED ENTITIES

- Update HIPAA compliance plan and policies and procedures
- Update policies and procedures for breach notification
  - Test risk assessment standard prior to compliance date
- Update policies for marketing, fundraising, and the sale of PHI
- Revise and distribute new Notice of Privacy Practices
- Update required authorization forms
- Assess encryption and de-identification capabilities
- Conduct updated workforce training
- Conduct risk assessment – technical, administrative, and physical safeguards
- Update EMR for flagging restricted PHI
- Update technology to provide patients with electronic access to PHI
- Bring BA Agreements and terms of subcontracts into compliance with updated requirements
  - Is the business associate acting as the agent of the covered entity?
- Confirm business associate compliance
  - Educate new business associates and subcontractors about HIPAA requirements
  - Confirm business associates' compliance with Security Rule: safeguards, policies and procedures, and documentation
  - Confirm business associates' compliance with relevant provisions of Privacy Rule
- Health Plans: Update underwriting policies to exclude genetic information

Because of the general nature of this *Update*, the information provided in the Update may not be applicable to all situations and should not be acted upon without specific legal advice based on particular circumstances.

---

[1] A "designated record set" is a group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.
