ALSTON & BIRD LLP

WWW.ALSTON.COM

Health Care ADVISORY ■

JANUARY 25, 2013

Overview of HIPAA/HITECH Act Omnibus Final Rule

On Friday, January 25, 2013, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) published the long-awaited 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" (Omnibus Rule), 78 Fed. Reg. 5566 (Jan. 25, 2013). The Omnibus Rule:

- finalizes modifications to the Privacy, Security, and Enforcement Rules to implement the Health Information Technology for Economic and Clinical Health (HITECH) Act, proposed in July 2010;
- finalizes modifications to the Privacy Rule, proposed in July 2010, to increase the workability of the Privacy Rule;
- modifies the Breach Notification Rule, adopted by interim final rule in August 2009; and
- finalizes modifications to the Privacy Rule to implement the Genetic Information Nondiscrimination Act of 2008 (GINA), proposed in October 2009.

This advisory provides a summary of the significant changes made by the Omnibus Rule in the Privacy, Security, Breach Notification and Enforcement Rules.[1]

I. COMPLIANCE PERIOD

The Omnibus Rule will be effective on March 26, 2013, with a compliance period of 180 days, requiring compliance as of September 23, 2013. In addition, the Omnibus Rule added a provision at 45 C.F.R. § 160.105 to provide a 180-day compliance period for new or modified HIPAA standards. HHS may extend this 180-day period for future modification when it determines additional time is warranted. With respect to the Omnibus Rule, the 180-day period does not apply to (1) the modifications to the Enforcement Rule, which are effective with the Omnibus Rule or as otherwise specified, and (2) provisions for which HHS expressly provides a different compliance period (such as the business associate agreement provisions).

---

[1] This advisory was written by Paula M. Stannard and Angela T. Burnette, who express their appreciation to the following Alston & Bird associates who assisted with this significant project: D'Andrea Morning, Kim McWhorter, Esther Yu, Trey Stephens, Guillermo Cuevas and Hannah Heck.

II. STATUTORY BASIS AND PURPOSE, APPLICABILITY, DEFINITIONS AND PREEMPTION OF STATE LAW, PART 160, SUBPARTS A-B

A. Applicability

HHS has added a new provision that makes it clear that certain provisions of the HIPAA Rules are applicable to business associates.

B. Definitions

Business Associate. HHS has expanded the definition of "business associate" at 45 C.F.R. § 160.103 to include patient safety organizations (PSOs), health information organizations (HIOs) and subcontractors. This expansion was issued to satisfy statutory provisions of the Patient Safety and Quality Improvement Act of 2005 (PSQIA), implement the HITECH Act, and avoid lapses in the applicability of the HIPAA regulations.

PSOs are required to be treated as business associates under the PSQIA, as these organizations receive and analyze protected health information (PHI) on behalf of covered health care providers. In its notice of proposed rulemaking (NPRM), HHS stated that a component PSO operating within a covered entity would not be considered a business associate, but a part of the workforce of the covered entity.

Also included as business associates are health information entities, such as HIOs, e-prescribing gateways, other persons that provide data transmission services or facilitate access to health records, and vendors of personal health records provided on behalf of covered entities. HHS considers this subcategory to encompass data transmission services requiring routine access to PHI and services that provide personal health records access on behalf of a covered entity. In the preamble to the Omnibus Rule, HHS stated there is a narrow exception for entities acting as mere conduits for transmitted information and that do not routinely access, store or maintain such information, but only on a random or infrequent basis as necessary to perform the transportation service or as required by law.

Lastly, under the Omnibus Rule, subcontractors (or agents) that perform services for a business associate are also considered business associates to the extent their services require access to PHI. A business associate is obligated to obtain satisfactory assurances from its HIPAA-covered subcontractors, in the form of a written agreement, that the subcontractor will appropriately safeguard the PHI. Entities that receive PHI only to assist a business associate with its own management and administration or legal responsibilities are not subcontractors (and, thus, not business associates). However, a business associate would be required to obtain reasonable assurances from such entities that the information would be held confidentially and only used or disclosed as required by law or for the purposes for which it was disclosed.

Electronic Media. The definition for electronic media has also been modified in 45 C.F.R. § 160.103 to reflect technological advances. Principally, the new definition (1) replaces the term "electronic storage media" with "electronic storage material," (2) expands the definition to include intranets, and (3) incorporates voice transmissions that were electronically stored prior to transmission. In addition, the preamble stated that devices that store PHI are subject to the Privacy and Security Rules regardless of whether such storage was intentional or not.

C. Preemption of State Law

HHS added references to section 264(c) of HIPAA and section 13421(a) of the HITECH Act that contain the statutory basis for the preemptive effect of the HIPAA Privacy Rule and the HITECH Act's privacy and security provisions. HHS stated that the congressional intent of the preemption provisions was to supersede only contrary provisions of state law; however, states can adopt more stringent privacy protections.

III. THE ENFORCEMENT RULE, PART 160, SUBPARTS C-D

A. Compliance and Enforcement

Under the Omnibus Rule's modifications, the Enforcement Rule provisions are more stringent than before. For example, under the modified 45 C.F.R. § 160.306(c), HHS will (as opposed to "may") investigate all complaints when evidence indicates a possible violation due to willful neglect. Similarly, HHS added an identical modification with respect to its compliance reviews under 45 C.F.R. § 160.308. According to the preamble, these revisions are intended to ensure that investigations are consistent regardless of whether they were initiated by a complaint or a compliance review. Significantly, HHS also removed the requirement that it first attempt informal resolution of investigations or compliance reviews, making such efforts voluntary. Now, under 45 C.F.R. § 160.312, HHS can proceed directly to imposition of civil monetary penalties (CMPs). Finally, 45 C.F.R. § 160.310 has been modified so that PHI collected in a compliance inquiry may be disclosed to another agency if such disclosure is permitted by law.

B. Imposition of CMPs

Reasonable Cause. Pursuant to the HITECH Act, HHS adopted changes to the Enforcement Rule, by interim final rule, to establish tiers of penalties based on the degree of culpability exhibited by the entity. The Omnibus Rule clarified the definition of "reasonable cause" as it pertains to the penalty tier for violations due to reasonable cause and not to willful neglect. The modified definition under 45 C.F.R. § 160.401 would encompass violations that were attributable to situations where (1) circumstances would make it unreasonable, despite the exercise of ordinary business care, to comply; or (2) an entity knows of a violation, but lacks the conscious intent associated with willful neglect. In an example provided by HHS, if a covered entity received an unusually high demand for access requests under 45 C.F.R. § 164.524(b)(2) and could not, despite its good faith efforts, meet the mandated time periods, the violation would be considered to be due to reasonable cause.

***Basis for a CMP*.** The Omnibus Rule removed an exception to liability for covered entities in 45 C.F.R. § 160.402(c) with respect to the acts of their agents.[2] Now, as a result of the Omnibus Rule, covered entities and business associates would be liable for activities of their agents, regardless of their own compliance. The preamble states that the scope of agency is determined by the federal common law standard, specifically looking at whether the covered entity or business associate had the right to control the agent's conduct. HHS also stated that a business associate of a covered entity is not ordinarily an agent; however, it can become one depending upon the context of the relationship, such as if the covered entity has the right to direct or control the business associate or where it contracts out or delegates a HIPAA obligation to its business associate.

---

[2] The exception applied where the agent is a business associate, the covered entity had complied with the business associate requirements of the HIPAA Rules and the covered entity did not (1) know of a pattern or practice of violations by the business associate and (2) fail to act as required by the HIPAA Rules with respect to such violations.

Amount of CMP and Factors Considered in Determining the Amount of Penalty. In the interim final rule, HHS enacted a tiered penalty scheme, located at 45 C.F.R. § 160.404, providing for monetary penalties based on culpability category (ranging from $100 to $50,000 per occurrence). Each category has the same maximum annual penalty - $1,500,000 - for all violations of a specific provision. In the Omnibus Rule, HHS stated that the number of occurrences or violations would be determined based on context, such as number of individuals affected by a data breach. Also, the Omnibus Rule included a list of factors at 45 C.F.R. § 160.408 to guide determination of the amount of the penalty. Factors include the nature and extent of the violation and its harm, as well as the general compliance history of the covered entity (previously, the covered entity's history of HIPAA violations had been considered).

IV. PRIVACY AND SECURITY: GENERAL PROVISIONS AND MODIFICATIONS TO THE SECURITY RULE, PART 164, SUBPARTS A AND C

A. Omnibus Rule Modifications to General Provisions

The Omnibus Rule made clear that, where indicated, the standards, requirements and implementation specifications of the HIPAA Privacy, Security, and Breach Notification Rules apply to business associates.

In regard to hybrid entities, the Omnibus Rule modifications require that the health care component of a hybrid entity include all business associate functions within the entity. Furthermore, the modifications clarify that the covered entity itself (and not merely the health care component) remains responsible for complying with the regulations (§§164.314 and 164.504) regarding business associate agreements and other organizational requirements. This means hybrid entities may need to execute legal contracts and conduct other organization matters at the level of the legal entity rather than at the level of the health care component.

B. Omnibus Rule Modifications to the Security Rule

Under the Omnibus Rule, business associates are now directly liable for compliance with the Security Rule. This means they must comply with the Security Rule's requirements for (1) administrative, physical and technical safeguards; (2) policies and procedures; and (3) documentation in the same manner as covered entities. Furthermore, business associates are civilly and criminally liable for violations of these provisions.

The Security Rule still permits flexibility of approaches to compliance and lists the factors a covered entity or business associate must consider in deciding which security measures to use. In addition, the modifications in section 164.306(e) clarify that covered entities and business associates must review and modify security measures as needed and update documentation of such security measures accordingly.

The Omnibus Rule revised the existing business associate agreement (BAA) requirements to now require a business associate to comply with the Security Rule, to ensure any subcontractors enter into a contract or other arrangement to protect the security of e-PHI, and report to the covered entity breaches of unsecured PHI. Moreover, the Omnibus Rule made the Security Rule BAA requirements applicable to arrangements involving a business associate and a subcontractor of that business associate in the same manner as the requirements apply to arrangements between covered entities and business associates. However, covered entities are not required to obtain satisfactory assurances from (or enter into a BAA with) a business associate that is a subcontractor; rather, this is the obligation of the business associate that has engaged the subcontractor.

V. MODIFICATIONS TO THE PRIVACY RULE, PART 164, SUBPART E

A. Applicability

Under the Omnibus Rule modifications, certain standards, requirements and implementation specifications of the HIPAA Privacy Rule now apply to business associates. Accordingly, a business associate is *directly* obligated to comply only with the following Privacy Rule requirements: (1) the prohibition on uses and disclosures of PHI that are not in accord with its BAA or the Privacy Rule; (2) the requirement to disclose PHI when required by the Secretary to do so and for failing to disclose PHI to the covered entity, individual or individual's designee, as necessary to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of PHI; (3) the requirement to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose; and (4) the requirement to enter into BAAs with its subcontractors that create or receive PHI on its behalf.

B. Definitions

Health Care Operations. The Omnibus Rule revised the definition of "health care operations" to include an express reference to patient safety activities in order to conform the Privacy Rule to the PSQIA and to the modified definition of "business associate" that includes PSOs.

Marketing. The Omnibus Rule significantly revises the definition of "marketing" and the exceptions to the definition. Previously, certain treatment and health care operations communications were excluded from the definition—even if the covered entity received financial remuneration for the communication—and, thus, the covered entity did not require authorization to make such communications. The new definition of "marketing" is such that it encompasses all treatment and health care operations communications where the covered entity (or business associate or subcontractor) receives financial remuneration for making such communications from a third party whose product or service is being marketed and, thus, requires prior authorization from the individual. Furthermore, all subsidized treatment communications that promote a health-related product or service will be treated as marketing communications that require authorization. The only exception to the definition of "marketing" that permits the covered entity (or business associate) to receive remuneration is for refill reminders and other communications about currently prescribed drugs or biologics, but only if any financial remuneration received in exchange for making the communication is reasonably related to the cost of making the communication. In the Omnibus Rule, HHS indicated that permissible costs for which a covered entity may receive remuneration under this exception are those that cover only the costs of labor, supplies and postage to make the communication; where the remuneration generates a profit, or includes payment for other costs, it would not meet the requirements of the exception. The term "financial remuneration" for purposes of the definition of marketing does not include non-financial benefits (e.g., in-kind benefits). It only includes those direct and indirect financial payments made in exchange for making communications about a product or service that encourages individuals to buy or use such product or service. The term does not include any payment for treatment of an individual.[3]

---

[3] HHS has preserved the exceptions to the requirement for authorization for remunerated marketing communications involving (1) face-to-face communications made by a covered entity to an individual; and (2) promotional gifts of nominal value provided by the covered entity.

C. Business Associates

Permitted and Required Uses and Disclosures. The Omnibus Rule adopted the proposed modifications to § 164.502(a), whereby business associates are permitted to use or disclose PHI only as permitted or required by their BAAs or other arrangements, or as required by law. They are prohibited from using or disclosing PHI in a manner that would violate the Privacy Rule if done by the covered entity (with exceptions for the proper management and administration of the business associate and to provide data aggregation services for the covered entity, if permitted by the BAA). Business associates are also directly required to (1) provide breach notification to the covered entity; (2) provide access to a copy of ePHI to either the covered entity, the individual or the individual's designee (whichever is specified in the BAA); (3) disclose PHI where required by the Secretary to investigate or determine the business associate's compliance with the HIPAA Rules; (4) provide an accounting of disclosures; and (5) comply with the requirements of the Security Rule.

Business associates are now directly liable for CMPs under the HIPAA Rules for violations of these requirements. The obligation to comply—and liability for compliance failures—will attach immediately when a person creates, receives, maintains or transmits PHI on behalf of a covered entity or business associate and otherwise meets the definition of a business associate, regardless of whether there is a BAA. Of course, business associates remain contractually liable for any obligations set forth in their BAAs.

Minimum Necessary. The Omnibus Rule modifications require business associates to comply with the minimum necessary standard when using or disclosing PHI or when requesting PHI from another covered entity or another business associate. Because of this requirement, covered entities and business associates disclosing PHI in response to a request from a business associate are permitted to reasonably rely on such requests as requesting the minimum necessary for the disclosure.

The Omnibus Rule contemplated that the manner in which a business associate will apply the minimum necessary standard will vary. While a business associate must be required, under its BAA, to limit its uses and disclosures of PHI consistent with the covered entity's minimum necessary policies and procedures, the Omnibus Rule allowed the parties to determine the extent to which the agreement specifies particular minimum necessary provisions to meet this requirement.

Business Associate Agreements. While section 13404 of the HITECH Act made business associates directly subject to some of the Privacy Rule requirements, there are still provisions of the Privacy Rule, such as providing a notice of privacy practices or designating a privacy official, to which business associates are not subject unless the covered entity has chosen to delegate such a responsibility to the business associate. (In such case, the business associate's obligation would be a contractual requirement for which contractual liability would attach.)

The Omnibus Rule modified § 164.502(e) to allow a business associate to disclose PHI to a business associate that is a subcontractor, and to allow the subcontractor to create or receive PHI on its behalf, if the business associate obtains satisfactory written assurances that the subcontractor will appropriately safeguard the information. Importantly, a *covered entity* is not required to obtain satisfactory assurances from business associates that are subcontractors, but the burden is instead placed on the *business associate* to obtain such assurances. Of course, the agreement between a business associate and a business associate that is a subcontractor may not permit the subcontractor to use or disclose PHI in a manner that would be impermissible if done by the business associate. Each agreement in the business associate chain must be as or more stringent than the one above it regarding the uses and disclosures of PHI.

Additionally, the Omnibus Rule modified § 164.504(e) with respect to the required contents of BAAs. Specifically, the Omnibus Rule:

- eliminated the requirement that covered entities report to the Secretary when it is not feasible to terminate a BAA, as would be required as a result of a business associate's material breach or violation of its obligations under the agreement;
- required a business associate that is aware of noncompliance by a subcontractor to respond to the situation in the same manner as a covered entity that is aware of noncompliance by its business associate;
- aligned the requirements for BAAs with the HITECH Act and other HIPAA requirements, so that the agreement would require a business associate (1) to comply with the applicable Security Rule provisions if it handles ePHI; (2) to report breaches of unsecured PHI to the covered entity, as required by the Breach Notification Rule; and (3) to ensure that any subcontractors that create or receive PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information; and
- where a business associate is to carry out a covered entity's obligation under the Privacy Rule, contractually require such business associate to comply with the Privacy Rule requirements applicable to the covered entity's obligation. While a business associate would be contractually liable to the covered entity for a failure to comply with such Privacy Rule requirements, only the covered entity would be directly liable for the Privacy Rule violation.

The Omnibus Rule modifications also directly require a business associate to enter into BAAs or other arrangements that comply with the Privacy and Security Rules with its business associate subcontractors, in the same manner that the covered entity is required to enter into a contract or other arrangement with it.

HHS noted that, despite a business associate's direct obligation to comply with certain provisions of the HIPAA Rules, the BAA is necessary to clarify and limit, as appropriate, the permissible uses and disclosures of PHI, given the relationship between the parties and the activities or services being performed by the business associate. HHS also indicated that the BAA is necessary to ensure that the business associate is contractually required to perform certain activities for which direct liability does not attach.[4]

Transition Provisions. The Omnibus Rule provided for a transition period for existing business associate agreements, grandfathering such agreements until September 22, 2014, at the latest. The transition period allows compliant business associate agreements that are in effect as of January 25, 2013, and are not renewed or modified between March 26 and September 23, 2013, to be deemed compliant until either the date that the agreement is renewed or modified, or September 22, 2014, whichever is earlier.

D. Authorizations

Sale of PHI. Under § 164.508 of the Privacy Rule, a covered entity may use and disclose PHI for purposes not otherwise permitted by that Rule, if the covered entity has obtained an authorization, which meets certain requirements, from the individual who is the subject of the PHI. An authorization must be obtained from the individual for (1) most uses and disclosure of psychotherapy notes; and (2) uses and disclosure for purposes of marketing. Under section 13405(d)(1) of the HITECH Act, a covered entity or business associate could not receive direct or indirect remuneration in exchange for the disclosure of PHI unless the covered entity had obtained an authorization consistent with § 164.508, which also

---

[4] A BAA is not necessary—and a data use agreement will suffice—when the business associate receives only a limited data set in order to carry out health care operations for the covered entity.

stated whether the PHI could be further exchanged for remuneration by the entity receiving PHI of that individual. Section 13405(d)(2) of the HITECH Act contained several exceptions. Generally, those HITECH Act exceptions included exchanges of PHI for purposes of public health activities, research, treatment of the individual, certain health care operations, to a business associate for certain activities involving the exchange of PHI (if certain criteria are met), to provide a copy of an individual's PHI under the Privacy Rule's access provisions, or as otherwise determined by the Secretary in regulations as similarly necessary and appropriate as the enumerated exceptions. Section 13405(d)(4) of the HITECH Act stated that the requirements with respect to the sale of PHI would apply to such exchanges of PHI occurring on or after the date six months after the date final regulations were promulgated.

The Omnibus Rule added §164.502(a)(5)(ii) to the Privacy Rule, which generally prohibits a sale of PHI by a covered entity or business associate absent an authorization from the individual in compliance with §164.508(a)(4). In response to commenters' requests, HHS provided a definition of "sale of protected health information" in §164.502(a)(5)(ii)(B)(1). That term is defined as "a disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI." HHS also provided significant discussion regarding the meaning of certain terms, including what is and is not a "sale," what is "direct or indirect" and what constitutes "remuneration."

As a general overview, a "sale" is not limited by HHS to those transactions in which there is a transfer of ownership of PHI, as suggested by commenters. As noted by HHS, the HITECH Act does not contain such a limitation; therefore, the sale provisions apply to disclosures of PHI in exchange for remuneration, including resulting from license, access or lease agreements. Similarly, a "sale" of PHI does not include the exchange of PHI through a Health Information Exchange (HIE), which is paid for through fees assessed on participants in the HIE; there, the remuneration is for the HIE's services rather than the data itself. HHS generally recognized that a "sale" of PHI occurs when the covered entity is primarily being compensated to supply data that it maintains in its role as a covered entity (or as a business associate). Additional examples are provided by HHS in the preamble regarding what constitutes a "sale." If the definition of a "sale" is met, an individual's authorization is required under §164.508(a)(4), and the authorization must state, in order to constitute a valid authorization, that the disclosure will result in remuneration to the covered entity.

HHS also clarified that the term "remuneration" is not limited to financial payment, but also applies to the receipt of nonfinancial benefits, including in-kind benefits. In this regard, the definition deviates from the definition applicable to the marketing provisions. Thus, according to HHS, a covered entity or business associate may not disclose PHI in exchange for in-kind benefits, unless the disclosure fits within an exception to the prohibition on the sale of PHI. HHS also noted that the terms "direct" and "indirect" establish that the prohibition applies to the receipt of remuneration from the third party that receives the PHI, as well as remuneration from another party on behalf of the recipient of the PHI.

HHS also added §164.502(a)(5)(ii)(B)(2), which delineates certain disclosures as not constituting a sale of PHI. These exceptions are set forth in more detail in the Omnibus Rule, along with specific other limitations/criteria relevant to a particular exception. Generally, these exclusions include disclosure of PHI (1) for certain public health purposes; (2) for certain research purposes; (3) for treatment and payment purposes (including disclosure of PHI to a collection agency for purposes of payment collection activities); (4) for the sale, transfer, merger or consolidation of all or part of the covered entity as further described and for related due diligence; (5) to or by a business associate for activities that the business associate undertakes on behalf of a covered entity (or on behalf of a business associate in the case of a subcontractor), and where the only remuneration provided is by the covered entity to the business associate (or by the business associate to the subcontractor), if applicable, for the performance of such activities; (6) to an individual exercising HIPAA access or accounting rights; (7) required by law; and (8) for any other purpose permitted by and in

accordance with applicable requirements of the Privacy Rule, if the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost of preparing and transmitting the PHI for such purpose or a fee otherwise expressly permitted by other law.

HHS addressed the business associate exception in some detail. HHS clarified that a business associate may recoup fees from third-party record requestors for preparing and transmitting PHI on behalf of a covered entity, if the fees were reasonable, cost-based fees to cover the cost of preparing and transmitting the PHI or as otherwise expressly authorized by other law. Also, HHS confirmed the business associate exception would include remuneration by a business associate to its subcontractor business associate for the subcontractor's activity performed on behalf of the business associate.

HHS also addressed commenters' questions as to redisclosures of PHI by a recipient covered entity or business associate. According to HHS, if a covered entity or business associate receives PHI for remuneration and wanted to further disclose that information in exchange for remuneration, then an additional authorization would be required. In that situation, the redisclosure would not be covered by the original authorization. However, HHS also noted that redisclosures of information for remuneration by a recipient covered entity or business associate might possibly not require additional authorization where it is sufficiently clear in the original authorization that the recipient covered entity or business associate will further disclose the individual's PHI in exchange for remuneration.

HHS also noted that a covered entity can rely on an authorization obtained prior to the compliance date, even if the authorization (whether for research or another purpose) did not mention the disclosure was in exchange for remuneration. Likewise, HHS clarified that a covered entity also can continue to rely on a waiver of authorization from an Institutional Review Board or Privacy Board obtained before the Omnibus Rule's compliance date. A covered entity also may continue to use or disclose a limited data set pursuant to a data use agreement until that agreement is renewed or modified as discussed further in the Omnibus Rule. HHS confirmed that the following are not implicated by the remuneration prohibition: (1) uses of PHI within a single covered entity or within a designated affiliated covered entity, and (2) disclosures of de-identified health information.

HHS also addressed what types of costs would be permitted as part of a reasonable cost-based fee. Such costs include those consistent with a state law fee schedule or as otherwise permitted by another law. Also, the permitted costs might include direct and indirect costs of preparing and transmitting the data. HHS reiterated, however, that fees charged to incur a profit from the disclosure of PHI are not permitted.

Compound Authorizations for Research Activities. The Privacy Rule generally prohibits compound authorizations, but also delineates some specific exceptions. One such exception includes the permitted combining of an authorization for a research study with any other written permission for the same research study (such as an informed consent to participate). However, the Privacy Rule also prohibited combining (1) an authorization that conditions treatment, payment, health plan enrollment or eligibility for benefits with (2) another authorization for a separate purpose for which treatment, payment, enrollment or eligibility cannot be conditioned. These two types of authorizations are referred to as conditioned and unconditioned authorizations, respectively. In the preamble to the Omnibus Rule, HHS noted commenters' concerns that these prohibitions have led to obtaining separate authorizations from research participants in clinical trials, which commenters urged was contrary to the Common Rule, burdensome and sometimes confusing to research subjects.

The Omnibus Rule amended § 164.508(b)(3)(i) and (iii) to allow a covered entity to use compound authorizations for conditioned and unconditioned research activities. Specifically, the Privacy Rule now permits an authorization for the use or disclosure of PHI for a research study to be combined with any other type of written permission for the same or another research study, including combining such an authorization with an authorization for the creation/maintenance

of a research database or repository or with a consent to participate in research. If a health care provider has conditioned research-related treatment on the provision of one of the authorizations (as permitted by HIPAA's Privacy Rule), then any such "compound authorization" is required to differentiate clearly between the conditioned and unconditioned research components and also must allow the individual the option to opt in to the unconditioned research activities.

These modifications do not remove the core elements or required statements of a HIPAA authorization, but a covered entity does have flexibility as to how it meets the authorization requirements; the preamble discusses various formats and approaches. HHS specifically declined to permit a compound authorization to contain only an option for the individual to "opt out" of the unconditioned research activities. HHS confirmed an individual must affirmatively authorize unconditioned research activities and specifically addressed scenarios involving revocation of compound authorizations.

Special consideration should be given to research that involves the use or disclosure of psychotherapy notes. Where research involves the use or disclosure of psychotherapy notes, an authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for psychotherapy notes, pursuant to the Privacy Rule.

The Omnibus Rule's modifications to § 164.508(b)(3(i) and (iii) permit, but do not require, covered entities to create compound authorizations for conditioned and unconditioned research activities. Thus, ongoing studies that were previously approved can continue to rely on the separate authorizations previously obtained. HHS notes that new research studies may choose to use separate authorizations for conditioned and unconditioned research activities or can move to using compound authorizations as described in the Omnibus Rule.

Authorizing Future Research Use or Disclosure. In the Omnibus Rule, HSS modified its interpretation of § 164.508(c)(1)(iv) of the HIPAA Privacy Rule, which required that an authorization for the use or disclosure of PHI include a description of each *purpose* of the requested use or disclosure. HHS had previously interpreted this provision as requiring that research authorizations be "study specific," limiting an individual's ability to agree to the use or disclosure of his or her PHI for future research. Under the modified interpretation set forth in the Omnibus Rule, an authorization for uses and disclosures of PHI for future research purposes may satisfy the requirements of § 164.508(c)(1)(iv) by adequate description, such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research. According to HHS, this modification brings the Privacy Rule interpretation in line with the current practice under the Common Rule.

HHS provided covered entities and researchers with flexibility in describing the information to be used or disclosed for the future research. However, it must be reasonable from the description that the individual would expect the information to be used or disclosed for future research. A description of the health information to be used in the future research may include information collected after the time of the original study.

This modified interpretation does not alter the HIPAA Privacy Rule's core elements or required statements of an authorization under § 164.508(c). For example, an authorization must list an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For research studies, an authorization may meet this requirement by listing a specific time period or a statement such as "the end of the research study," "none," or similar language.

If a covered entity wishes to obtain individual authorization for the use or disclosure of PHI for future research, it may do so after the effective date of the Omnibus Rule. In the alternative, a covered entity may choose to use its study specific authorization forms for research. In commentary, HHS noted that a covered entity and researchers can rely on IRB-approved consent obtained before the effective date of the Omnibus Rule, if that consent reasonably informed individuals of the future research and was combined with a HIPAA authorization.

E. Decedents

Period of Protection. The Omnibus Rule amended § 164.502(f) of the HIPAA Privacy Rule and now limits - to 50 years following the individual's date of death - the period during which a covered entity must comply with the Privacy Rule regarding a decedent's PHI. Previously, § 164.502(f) contained no time period and generally stated that a covered entity must comply with the HIPAA Privacy Rule regarding a deceased individual's PHI.

HHS emphasized that the 50-year period of protection for decedent health information does not override or interfere with state or other laws that provide greater protection for decedent health information (such as regarding HIV/AIDS, substance abuse or mental health) or providers' professional responsibilities. HHS noted that covered entities may continue to provide privacy protections to decedent information beyond the 50-year period, and may be required to do so under other applicable laws or as part of their professional responsibilities.

HHS also confirmed that the Omnibus Rule did not create a new 50-year record retention requirement. Covered entities may destroy medical records at the time permitted by state or other applicable law. However, if a covered entity does maintain decedent health information for longer than 50 years following the date of the individual's death, the Omnibus Rule states this information will no longer be subject to the Privacy Rule.

Disclosures to Family Members and Others Involved in Care. The Omnibus Rule added a new subsection (5) to § 164.510(b) of the Privacy Rule regarding uses and disclosures for involvement in the individual's care and notification purposes. As a result of the Omnibus Rule, the Privacy Rule now expressly permits covered entities to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so would be inconsistent with the individual's prior expressed preference, which is known to the covered entity. As with the other disclosures permitted under § 164.510(b), the Privacy Rule limits such disclosures to the information relevant to the family member or other person's involvement in the individual's health care or payment for health care.

HHS has interpreted the phrase "involved in the individual's care" as requiring the same level of proof as that required with respect to disclosures of PHI of living individuals under § 164.510(b): that is, subject to certain conditions, a covered entity may make a disclosure under this provision if it has *reasonable assurance* that the family member or other person was involved in the individual's care or payment for care prior to death.

HHS reiterated that while these disclosures are permitted, they are not required. Accordingly, if a covered entity questions the relationship of the person to the decedent or, based on the circumstances, is uncomfortable or otherwise believes that disclosure of the decedent's PHI would not be appropriate, the covered entity is not required to make such disclosure. Additionally, HHS clarified that this new subsection (5) would not alter other Privacy Rule provisions that also permit the use or disclosure of a decedent's PHI, such as provisions regarding personal representatives, public health authorities and law enforcement officials.

F. Disclosure of Student Immunizations to Schools

HHS noted the important role schools play in preventing communicable diseases and that most states have laws that prohibit a student from attending school unless the school has received the student's immunization records. Accordingly, the Omnibus Rule amended § 164.512(b)(1) of the Privacy Rule, regarding public health activities. The Omnibus Rule added a new paragraph that permits a covered entity to disclose proof of immunization to a school where state or other law requires the school to have such information prior to admitting the student. Written authorizations are no longer required to permit this type of disclosure, but covered entities must still obtain an agreement, which may be oral and

over the phone, from a parent, guardian or other person acting *in loco parentis* for the individual, or directly from the individual, if he or she is an adult or emancipated minor. The agreement is considered effective until revoked.

The Omnibus Rule also required that covered entities document the agreement obtained under this provision. The Omnibus Rule provided covered entities some flexibility and does not dictate the nature of the documentation or require a parent's signature. HHS noted the documentation must only make clear that agreement was obtained as permitted under this new provision. In requiring active agreement, HHS declined to presume such disclosures would be permitted and specifically declined to provide an opt-out format. HHS also noted this new provision would not permit disclosure by a covered entity in response to a request *from the school* (as compared to a request from the parent or guardian).

However, the Privacy Rule at § 164.512(a) permits a covered entity to use or disclose PHI to the extent required by law, if the use or disclosure complies with, and is limited to, the relevant requirements of such law, or for public health activities (such as immunization registries). The Privacy Rule does not prohibit immunization disclosures that are *required* by state law, nor does it require authorizations for such disclosures. However, where state laws *permit*, but do not require, covered entities to disclose immunization records to schools, the disclosures would not be required by law and, thus, § 164.512(a) could not be used as the basis for disclosure. Such disclosures would have to meet the agreement and documentation requirements contained in the new section summarized above.

Additionally, HHS noted that once immunization records are obtained and maintained by the school, those records are protected by the Family Educational Rights and Privacy Act (FERPA), rather than by the Privacy Rule.

G. Fundraising

The Omnibus Rule specifically addressed the use and disclosure of PHI for fundraising communications and stated it generally adopts previously proposed language.

The Omnibus Rule did not change the types of communications currently considered to be for fundraising purposes under the Privacy Rule. That is, the following communications are still considered fundraising communications: a communication to an individual that is made by a covered entity, an institutionally related foundation or a business associate on behalf of the covered entity for the purpose of raising funds for the covered entity. 45 C.F.R. §164.514(f). HHS noted that the Privacy Rule has always required that fundraising communications describe how the individual may opt out of receiving further fundraising communications. In issuing the Rule, HHS specifically declined to provide an *opt-in* process, noting it would be inconsistent with the HITECH Act's provisions that provide for opting out of fundraising communications. HHS also reiterated that the notice and opt-out requirements would be inapplicable if a covered entity does not use PHI to target the fundraising communication. For example, the HIPAA notice and opt-out requirements would not apply if a covered entity used a public directory to mail fundraising communications to all individuals who reside in a particular geographic area.

Generally, with the Omnibus Rule, HHS sought to strengthen individual rights consistent with the HITECH Act, but also provide covered entities with flexibility regarding fundraising communications. As summarized below, this flexibility includes how covered entities permit individuals to opt out of fundraising communications and whether the opt-out choice applies to all fundraising communications or a specific fundraising campaign. The Omnibus Rule also expanded, to some degree, the scope of information a covered entity may decide to use in targeting fundraising communications. There are also specific restrictions and requirements now in place. For example, a covered entity may not condition an individual's treatment or payment on whether the individual opts out of fundraising

communications. A covered entity may not send fundraising communications to an individual who has opted out of receiving such communications. Also, covered entities that make fundraising communications by phone must clearly inform individuals they have a right to opt out of further solicitations.

Regarding fundraising opt-out methods, HHS emphasized that the opt-out methods chosen by the covered entity cannot impose an undue burden or more than a nominal cost upon the individuals. For example, covered entities could use a toll-free phone number, an e-mail address or similar opt-out mechanisms if they provide individuals with simple, quick and inexpensive ways to opt out of receiving additional fundraising communications. Covered entities may also decide to use a single (uniform) opt-out method if that method is reasonably accessible to all individuals who wish to opt out. Alternatively, covered entities may decide to provide multiple opt-out methods, and the individuals can decide which opt-out method is the simplest and most convenient for them. HHS encouraged covered entities to consider the size and geographic distribution of the population involved when assessing and choosing which opt-out method(s) are most appropriate and least burdensome for those individuals. Of note, HHS is still considering whether a covered entity's requirement for individuals to *write and send* a letter to the covered entity asking not to receive further fundraising communications may constitute an undue burden. HHS expressly confirmed that a covered entity's requirement for individuals to opt out by mailing back a *pre-printed, pre-paid postcard* would not be an undue burden.

Under the Omnibus Rule, HHS provided covered entities with discretion as to the scope of the opt-out provided to individuals for fundraising communications - e.g., whether an opt-out for all fundraising communications or an opt-out for a specific fundraising campaign. If a covered entity is concerned with the ability or burden of tracking campaign-specific opt-outs, HHS notes a covered entity can apply an individual's opt-out to all future fundraising communications. On the other hand, if a covered entity chooses to, *and* has the ability to track campaign-specific opt-outs, the covered entity may apply the opt-out only to specific fundraising campaigns. Covered entities also can provide individuals with two choices: (1) opting out of all future fundraising communications *or* (2) opting out of fundraising communications regarding specific campaigns. Regardless of the opt-out method utilized by the covered entity, the communication should clearly inform individuals about their opt-out choices and the consequences of choosing to opt out of further fundraising communications.

Also, under the Omnibus Rule, if individuals have opted out of future fundraising communications, then covered entities are now *prohibited* from sending them further fundraising communications, as compared to covered entities previously using "reasonable efforts" so that individuals who opted out do not receive such communications. HHS noted commenters' concerns about "lag times," updating of mailing lists and other administrative difficulties in tracking which individuals have opted out of further fundraising communications. However, consistent with the HITECH Act, an individual's opt-out of fundraising communications must now be treated as a revocation of a HIPAA authorization, and HHS noted that covered entities already must track which individuals have revoked authorizations. HHS expects a covered entity to use the same care and attention in how it handles PHI for fundraising communications as it uses in its health care operations. According to HHS, if a covered entity elects to send fundraising communications to individuals, then the covered entity must have data management systems and processes in place to timely track and flag those individuals who have opted out, so they do not receive additional fundraising communications.

The Omnibus Rule also provided a covered entity with discretion in determining how individuals should be able to opt back in to receive the covered entity's fundraising communications. While HHS expressly declined to permit an individual's opt-out to automatically lapse over time, HHS recognized a covered entity could include in a routine newsletter to all patients a phone number they could call if they wished to be placed on the covered entity's fundraising list. Similar to an individual actively deciding to opt out, HHS emphasized that an individual's "active" decision would suffice to opt back in, after previously opting out of fundraising communications.

Many commenters asked HHS to clarify the Privacy Rule provision permitting a covered entity to use an individual's demographic information for fundraising communications. The Omnibus Rule clarified that such permitted demographic information may include names, addresses, other contact information, age, gender and dates of birth. Also, covered entities may use or disclose information about an individual's health insurance status for fundraising purposes, but HHS listed that category of information separately because it did not consider that to be "demographic information." Additionally, in response to comments regarding the need for covered entities to target fundraising communications to appropriate individuals, the Rule now permits covered entities to use and disclose the following information of an individual for fundraising purposes: (1) department of service information (e.g., the general department of treatment, such as cardiology, oncology or pediatrics); (2) treating physician information; and (3) outcome information (including information regarding the patient's death or any sub-optimal result of treatment or services). HHS expressly intends a covered entity to use the outcome information to screen and remove from fundraising solicitations those individuals who experienced a sub-optimum outcome.

A covered entity's notice of privacy practices still must inform individuals that it may contact them for fundraising purposes and that they have a right to opt out of receiving such communications. Because individuals will receive clear notice of their ability to opt out of fundraising communications, both in the covered entity's notice of privacy practices and the first fundraising communication, HHS declined to required covered entities to send pre-solicitation opt-outs to individuals before the first fundraising communication.

H. Notice of Privacy Practices (NPP)

Under § 164.520 of the Privacy Rule, most covered entities are required to have and distribute an NPP that, among other things, describes permitted uses and disclosures of PHI and summarizes individuals' rights regarding their PHI.

The Omnibus Rule modified § 164.520 to require the addition of several statements to a covered entity's NPP. First, an NPP must now contain a statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require authorization. HHS clarified, however, that the required NPP statement regarding authorizations for psychotherapy notes is inapplicable to covered entities that do not record or maintain psychotherapy notes. Second, a NPP must state that other uses and disclosures not described in the NPP will be made only with authorization from the individual. Third, if a covered entity intends to contact the individual for fundraising purposes, the NPP must now contain a statement informing the individual of this intention and of his or her right to opt out of receiving such fundraising communications. HHS clarified that a covered entity is not required to state in its NPP the specific mechanism for opting out of receiving fundraising communications, but the covered entity can do so if it wishes. Fourth, the NPP must now contain a statement informing the individual of his or her right to restrict disclosures of PHI to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full; however, HHS noted this new NPP requirement would only apply to health care providers' NPPs. Other covered entities may use existing NPP language, which states that a covered entity is not required to agree to a requested restriction. Fifth, the NPP must now contain a statement explaining the right of affected individuals to be notified following a breach of unsecured PHI. HHS confirmed that a simple statement set forth in an NPP (e.g., an individual has a right to or will receive notifications of breaches of his or her unsecured PHI), will sufficiently comply with this new requirement.

HHS also confirmed that the Omnibus Rule's required revisions to NPPs constitute "material changes" to covered entities' NPPs. Accordingly, HHS confirmed that these material changes trigger distribution obligations. The Omnibus Rule modified § 164.520(c) to alter the distribution requirements for health plans. Now, under the Omnibus Rule,

a health plan that currently posts its NPP on its website must: (1) prominently post the material change or its revised NPP on its website by the effective date of the material change to the NPP (e.g., the compliance date of the Omnibus Rule); and (2) provide the revised NPP, or information about the material change and how to obtain the revised notice, in the health plan's next annual mailing to individuals then covered by the plan. For example, this mailing could take place at the beginning of the plan year or during an open enrollment period. 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 individuals covered by the plan within 60 days of the material revisions to the NPP. HHS specifically noted that health plans have the burden to provide revised NPPs, and both paper-based and web-based NPPs should be provided in a manner accessible to all beneficiaries, including disabled individuals.

The Omnibus Rule did not, however, revise the current distribution obligations regarding revised NPPs of health care providers who have a direct treatment relationship with an individual. Those health care providers must make the NPP available upon request on or after the revision's effective date, must have the NPP available at the delivery site and must post the notice in a clear and prominent location. HHS confirmed that health care providers need not print and hand out a revised NPP to all individuals; also, health care providers may post a summary of the NPP in a clear and prominent location at the delivery site, if the full NPP is immediately available, such as on a table directly below the posted summary. HHS cautioned that a copy of the full NPP should be immediately available to patients without imposing additional burden on the individual patients. Thus, HHS noted, it would be inappropriate to require an individual to ask for a copy of the full NPP in order to receive it. Also, HHS stated that covered entities may distribute NPPs or notices of material changes by email to an individual, if he or she has agreed to receive an electronic copy. HHS also reminded health care providers that they must provide a copy of the NPP to, and obtain a good faith acknowledgement of NPP receipt from, *new* patients.

HHS also addressed a covered entity's obligations under the Omnibus Rule if it had already revised its NPP in response to the HITECH Act or state law requirements. According to HHS, as long as a covered entity's current NPP is consistent with the Omnibus Rule and individuals have been informed of all material revisions made to the NPP, that covered entity would not be required to revise and distribute another NPP as a result of the Omnibus Rule's publication. Readers are cautioned that the Omnibus Rule contains several important changes to numerous HIPAA Privacy Rule provisions. Legal review of a covered entity's current NPP is encouraged and can help to confirm whether a current NPP is consistent with the Omnibus Rule, in order to determine whether a covered entity can take advantage of this opportunity.

HHS noted that there is no "one-size-fits-all" approach to NPPs and that each NPP will vary based on a particular covered entity's functions. HHS emphasized, though, that covered entities that must comply with Section 504 of the Rehabilitation Act of 1973, the Americans with Disabilities Act or Title VI of the Civil Rights Act of 1964 may have additional obligations to ensure effective communication and meaningful access regarding NPPs.

I. Right to Request Restrictions

Under §164.522(a) of the Privacy Rule, a covered entity must permit an individual to *request* that the covered entity restrict certain uses or disclosures of PHI about the individual: (1) to carry out treatment, payment or health care operations; and (2) to persons involved in the individual's care. While a covered entity is not required to agree to such a request, if the covered entity agrees to the restriction request, it must abide by the restriction except for emergency treatment purposes. The Privacy Rule also addressed a covered entity's termination of an agreed-upon restriction and documentation requirements. Although a covered entity previously had discretion whether to agree to an individual's requested restriction of PHI, under the Omnibus Rule, a covered entity, consistent with section 13405(a) of the HITECH

Act, *must now agree* to a specific type of restriction request, if certain criteria are met. Under the Omnibus Rule, a covered entity also must document restrictions according to 45 C.F.R. § 160.530(j).

Under the Omnibus Rule, in a new subsection (vi) added to § 164.522(a)(1), a covered entity must honor an individual's request to restrict disclosure of his or her PHI to a health plan if (1) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law *and* (2) the PHI pertains solely to a health care item or service for which the individual, or a person other than the health plan on behalf of the individual (such as a family member), has paid the covered entity in full. HHS realized this new subsection would, in effect, apply only to HIPAA covered health care providers and only to their disclosures to health plans.

HHS noted that disclosures required by law are exempt from this requirement, such as disclosures required for Medicare and Medicaid audits, Medicare conditions of participation regarding health care providers, court orders and other legally mandated disclosures. If state or other law requires that a health care provider submit a claim to a health plan for a covered service provided and does not allow an exception or procedure for those individuals who wish to pay out of pocket, the disclosure of PHI is considered legally mandated and would be exempt from the new mandatory restriction obligation. HHS noted that Medicare appears to contain such an exception, under which a Medicare beneficiary (or a beneficiary's legal representative) can refuse to authorize the submission of a bill to Medicare and instead pay out of pocket for the service. In that instance, a covered entity is not required to submit the claim to Medicare and must agree to such beneficiary's requested restriction to Medicare regarding that service (because the submission of that claim is not required by law).

While the Omnibus Rule did not require that health care providers create separate medical records, HHS noted providers would need to flag restricted records to prevent inadvertent disclosure or access to a health plan, such as during a health plan audit. HHS also noted a provider cannot notify a business associate of a health plan if it is restricted from notifying the health plan.

HHS provided significant clarifications with respect to how the new restriction obligation in (vi) would play out in different situations, including as to a bundle of health care services provided in one patient encounter, downstream providers, health care providers' counseling and assistance to patients, follow-up care obtained by a patient and out-of-network care. HHS also provided clarification as to how a covered health care provider should proceed if an individual's payment to the provider (a necessary part of the restriction obligation) is dishonored (e.g., the patient's check bounces).

The Omnibus Rule clarifies in § 164.522(a)(2) that a covered entity may still terminate a restriction upon notice to the individual; however, the covered entity cannot unilaterally terminate a mandatory restriction if the individual has met the requirements of the new mandatory restriction, set forth above. HHS retained language in §164.522(a)(2) that a provider may only terminate the restriction effective for PHI created or received after the covered entity notified the individual of the termination.

J. Right to Access

Under Section 164.524 of the HIPAA Privacy Rule, individuals have a right to request access or obtain copies of their PHI as maintained in designated record sets. The HITECH Act strengthens individuals' access rights regarding electronic health records (EHRs). Significantly, the Omnibus Rule expanded individual access rights under HIPAA to PHI maintained electronically in one or more designated record sets, *whether or not the designated record set is an EHR*. The Omnibus Rule also addressed the form and format of these access requests, the form and format of PHI provided in response to such requests, disclosure of PHI to third parties upon an individual's request, the fees a covered entity may charge and the timeframes within which a covered entity must respond to an access request.

Form/Format. The Omnibus Rule adopted the proposal to amend the Privacy Rule at §164.524(c)(2)(ii) to require that if an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if that is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. HHS stated in the preamble it expected covered entities to provide individuals with a "machine readable" copy of the PHI, which would include an electronic copy of the PHI in the following formats: MS Word, Excel, text, HTML or text-based PDF. HHS noted that what constitutes a readable electronic form and format will vary from system to system, covered entities will likely update their technology over time, and covered entities have flexibility in providing readily producible electronic copies of PHI as currently available on their systems.

HHS also confirmed individuals do not have unlimited choices in the type of electronic copies of PHI they request and that covered entities need not buy new software or systems to accommodate a request for a specific form not readily producible at that time, if the covered entity can provide some readable electronic copy. HHS noted that a PDF is widely recognized and could be used to satisfy the electronic access requirement if the individual requested the PHI in a PDF format or if the individual agreed to accept the PDF. If, however, the individual chose not to accept any of the electronic formats offered by the covered entity, then the covered entity must provide a hard copy of the PHI.

While most commenters opposed the proposal to expand individual access to all electronic designated record sets rather than just to EHRs, HHS determined that it had the authority to expand the access requirement in that manner. HHS anticipated any additional burden to covered entities would be small because individual access rights already applied to PHI in both paper and electronic designated record sets. Additionally, in response to comments, HHS clarified that covered entities would not need to compromise their data security by allowing individuals to have direct access to the system; instead, covered entities must provide individuals with an electronic *copy* of their PHI. HHS also noted that the business associate agreements between a covered entity and a business associate will govern as to a business associate's obligations, if any, to assist the covered entity in meeting its obligations to provide individuals with electronic access to their PHI.

HHS also provided significant clarification on a number of issues, including the format of the individual's request, the content and scope of PHI a covered entity must provide in response, the use of external portable media (such as a flash drive) on a covered entity's system and the covered entity's use of unencrypted email.

Third-Party Disclosure. Under the HITECH Act, an individual could choose to request that a covered entity directly send the copy of PHI to a third party, if the individual's specific request is in writing, signed by the individual and clearly designates the third party to whom the covered entity should send the PHI. The Omnibus Rule amended the Privacy Rule to state that a covered entity, if requested by an individual, *must* transmit the requested copy of PHI directly to a designated person, if the individual's request (1) is in writing; (2) is signed by the individual; and (3) clearly identifies the designated person and where the covered entity should send the PHI. In response to comments, HHS clarified that covered entities can rely on information provided in writing by the requesting individual, but also must still implement reasonable procedures to verify identity under § 164.514(h) and implement reasonable safeguards under § 164.530(c).

Fees. The Privacy Rule's access provision permits a covered entity to charge an individual a reasonable cost-based fee for providing copies of PHI pursuant to the individual's right to access. Under the HITECH Act, provision of an electronic copy of PHI from an EHR cannot include a charge by the covered entity for more than its labor costs in responding to the request. Now, under the Omnibus Rule, the reasonable fee that may be charged for providing the requested PHI, whether in paper or electronic form, specifically includes certain labor and supply costs as set forth in more detail in the Omnibus Rule.

In response to comments, HHS explained that the labor cost would include skilled technical staff time creating and copying the electronic file or preparing an explanation or summary of the file if applicable. HHS further clarified that reasonable supply costs would involve creation of paper or electronic media, but would *not* include a retrieval fee, the cost of obtaining new types of technology to respond to requests or fees for maintaining data access and infrastructure. Additionally, HHS noted that if state law specified or limited the fees to be charged, then the covered entity could only charge the lesser of the reasonable cost-based amount or the amount allowed by state law.

Timeliness. The Omnibus Rule also modified the time periods for a covered entity to respond to requests for access. Under the Omnibus Rule, an individual's access request for electronic and/or hard copies of PHI must be responded to by the covered entity within 30 days. If the information cannot be gathered within the initial 30-day period, then the covered entity may obtain a one-time extension of 30 days when necessary, if it provides the individual with written notice of the reasons for the delay and the expected date by which the covered entity will complete its action on the individual's request. The Omnibus Rule thus shortened the time period (from 90 days down to 60 days) for a covered entity to respond to access requests for information not maintained or accessible to the covered entity on-site. HHS declined to issue separate timeframes for responding to paper or electronic access requests. HHS also specifically declined to provide a transition period for covered entities; HHS did not believe additional time was necessary since covered entities must produce electronic copies of PHI that are readily producible.

VI. MODIFICATIONS TO THE BREACH NOTIFICATION RULE

The HITECH Act establishes several notification requirements for covered entities and business associates following the discovery of a breach of unsecured PHI. On August 24, 2009, HHS issued interim final regulations implementing the HITECH Act breach notification requirements (the "Interim Final Rule"), effective on September 23, 2009, and codified at 45 C.F.R. Part 164, Subpart D as the Breach Notification Rule. Under the Breach Notification Rule, covered entities are required to provide notification to each affected individual whose unsecured PHI was impermissibly used or disclosed, to the Secretary of HHS, and in some cases, to media outlets. Business associates are required to provide notice of a breach of unsecured PHI to covered entities.[5] In the Omnibus Rule, HHS made significant changes to the Breach Notification Rule's definition of "breach" and provided guidance on a number of Breach Notification Rule issues.

The Interim Final Rule defined a breach as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the PHI."[6] For purposes of the definition of breach, the Interim Final Rule defined "compromises the security or privacy of PHI" to mean "poses a significant risk of financial, reputational, or other harm to the individual" (i.e., the harm standard). It was intended to align the HIPAA/HITECH Act breach notification requirement with other federal and state breach notification laws. HHS indicated in the preamble to the Interim Final Rule that, in order for a covered entity or business associate to determine whether an impermissible use or disclosure of PHI constituted a breach, it must perform a risk assessment to determine if there was a significant risk of harm to the individual resulting from the impermissible use or disclosure.

---

[5] This advisory focuses on the Omnibus Rule's changes to the Breach Notification Rule. For a detailed discussion of the Breach Notification Rule, readers are directed to Alston & Bird's August 24, 2009, *Health Care Advisory*, "The Duty to Warn: The New HHS Breach Notification Requirements," which may be found at www.alston.com.

[6] 45 C.F.R. § 164.402 (Interim Final Rule).

Definition of Breach. Under the Omnibus Rule, HHS amended § 164.402 to modify significantly the definition of "breach" and the risk assessment approach. HHS stated that the definition in the Interim Final Rule and language in its preamble could be misconstrued and implemented incorrectly and therefore made the following changes.

- HHS added to the definition of "breach" that an impermissible acquisition, access, or use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate "demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment." HHS believed breach notification necessary in all situations unless that demonstration is made (or another exception to the definition of breach applies). Through this clarification, HHS seeks to ensure that the regulations are interpreted and applied in a uniform manner among all covered entities and business associates.
- HHS removed the harm standard and modified the risk assessment requirement to focus more objectively and uniformly, rather than subjectively, on the probability that PHI has been compromised. Under the new language in the Omnibus Rule, breach notification is not required if a covered entity or business associate can demonstrate through a risk assessment that a low probability exists that the PHI has been compromised, rather than demonstrating that there is no significant risk of harm to the individual (as under the Interim Final Rule).
- HHS recognized that the risk assessment approach is necessary in determining whether notification is required. The following factors must be considered by covered entities or business associates as they assess the probability of whether PHI was compromised: (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 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. HHS noted that, depending on the circumstances, it may be appropriate to consider other factors in the risk assessment. HHS expects all risk assessments to be thorough and completed in good faith, and for entities to reach reasonable conclusions.
- HHS eliminated the exception for limited data sets not containing dates of birth or zip codes. Under the Omnibus Rule modifications, a risk assessment must be performed after the impermissible use or disclosure of any PHI, including limited data sets, in order to determine if breach notification is required. HHS retained the other exceptions to the definition of "breach," and noted that the applicability of a breach exception to an incident must be judged at the time the incident is discovered and evaluated. When an exception is found to apply, there is no breach, and neither risk assessment nor notification is required. Covered entities or business associates should take necessary steps to ensure that the information is not subject to further impermissible use or disclosure. If, however, the information is further impermissibly used or disclosed, the subsequent use or disclosure should be treated as a separate incident for which separate evaluation is required.

HHS encouraged covered entities and business associates to take advantage of the breach notification safe harbor provision by encrypting PHI and limited data sets in accordance with the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals. PHI encrypted in accordance with this guidance is considered secured, and breach notification is not required following an impermissible use or disclosure of this information.

HHS also advised covered entities and business associates to (1) update their policies and procedures to reflect the changes to the definition of breach, including the specific requirements for risk assessment, and other changes to the breach notification rule; and (2) retrain workforce members, as appropriate, regarding these regulatory changes and any internal policies and procedure changes.

Notification to Individuals. In the Omnibus Rule, HHS provided guidance on notification to individuals. It noted that covered entities are ultimately responsible for notifying affected individuals of a breach, although covered entities are allowed to delegate the responsibility to the business associate that caused the breach or to another of its business associates. A covered entity and its business associate should evaluate which one is in the best position to provide the required notice to the affected individual. This evaluation may depend on a number of factors, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual. Also, when multiple covered entities participate in a Health Information Organization (HIO) and a breach occurs there, the notification obligation remains with the covered entities. Where it is difficult to determine which covered entities' individuals are affected by the breach, the HIO may have to notify all potentially affected covered entities. The covered entities may in turn delegate to the HIO the responsibility to notify the affected individuals. HHS also advised that, consistent with the Privacy Rule's provision for confidential communications, including alternate means or at alternate locations, breach notifications may be sent to individuals at alternative addresses, if the individuals requested communications be sent to the alternative addresses. Additionally, notification may be provided orally or by telephone, in limited circumstances, where the individual has requested to only receive communication in this manner, but declines to pick up the written breach notification. In such circumstance, HHS will exercise enforcement discretion with respect to the requirement to provide written notification.

Notification to the Media. HHS also provided clarifying guidance on three issues relating to notice to the media. First, a covered entity is not required to incur any cost to print or run a media notice. Second, prominent media outlets which receive the notification are not obligated to print or run information about the breach. Third, the posting of a press release on a covered entity's website does not fulfill the requirements for media notification; the required notification must be provided directly to the media outlet where the affected individuals reside.

Notification to the Secretary of HHS. HHS modified the Breach Notification Rule to clarify that covered entities must notify the Secretary of all breaches of unsecured PHI affecting fewer than 500 individuals no later than 60 days after the end of the calendar year in which the breaches were discovered, not the year in which the breaches *occurred*. On the issue of "immediately" reporting breaches involving 500 or more individuals, HHS noted that immediate reporting requires the covered entity to notify the Secretary contemporaneously with its notice to the affected individuals.

Notification by a Business Associate. In the Omnibus Rule, HHS noted that where a business associate is acting as an agent of a covered entity, under the federal common law of agency, the business associate's discovery of the breach will be attributed to the covered entity. In such case, the covered entity will be required to provide notification based on when the business associate discovered the breach, not when the business associate notifies the covered entity. However, if the business associate is not an agent, then the covered entity is required to provide notification based on the time when it is notified of the breach by the business associate. HHS also encouraged covered entities and business associates to address the timing of notification in their BAAs.

Enforcement. HHS addressed commenters' questions regarding OCR's enforcement authority under the Breach Notification Rule. HHS confirmed that OCR is permitted to enforce the breach notification rule pursuant to its authority under the Enforcement Rule and may impose CMPs against those entities failing to comply with the breach notification requirements. OCR also has the authority to work with covered entities to achieve voluntary compliance through informal resolution, except in cases involving willful neglect. Additionally, because each breach of unsecured PHI involves an impermissible use or disclosure in violation of the Privacy Rule, OCR may also impose a CMP for the underlying Privacy Rule violation, even in cases where the breach notification requirements are met.

Other Breach Notification Issues. HHS reminded covered entities and business associates that they can provide breach notification following any impermissible use or disclosure of PHI without performing a risk assessment. HHS reiterated the importance of workforce member training regarding breaches, as well as on the policies and procedures for reporting, evaluating and documenting breaches of unsecured PHI. HHS stated that it believes covered entities will be able to comply with both state and federal requirements regarding breach notification with one breach notice, given the flexibility of requirements in the breach notification rule.

VII. MODIFICATIONS TO THE PRIVACY RULE UNDER GINA

Section 105 of the Genetic Information Nondiscrimination Act of 2008 (GINA) requires HHS to amend the Privacy Rule to explicitly state that "genetic information" is PHI and to prohibit certain health plans from using genetic information for underwriting purposes. The Omnibus Rule implemented those requirements. It amended the definition of health information in 45 CFR § 160.103 to include "genetic information," which is also defined in that section. Exercising its general HIPAA authority, as well as its authority under GINA, HHS amended the Privacy Rule's general rules on the uses and disclosures of PHI (section 164.502) to prohibit all health plans, with the exception of long-term care policy insurers, from using or disclosing an individual's PHI that is genetic information for underwriting purposes.[7] The Omnibus Rule specifically excludes long-term care plans from the underwriting prohibition based on many comments, received in response to the proposed rule, that a blanket prohibition on all health insurance issuers would have a potential negative impact on a long-term care insurer's ability to effectively underwrite such policies and, thus, on the economic viability of the long-term care insurance market.

The prohibition in the Omnibus Rule applies to all genetic information from the compliance date of Omnibus Rule, regardless of when or where the genetic information originated. In defining "genetic information," HHS made it clear that, while information concerning the manifestation of a disease or condition in a family member constitutes "genetic information" about an individual, information concerning the manifestation of a disease or condition in the individual does not constitute "genetic information" with respect to that individual. Thus, information concerning a disease or condition that has manifested itself in an individual (but not similar information concerning a manifested disease of a family member) can be used for underwriting purposes with respect to that individual.[8] Furthermore, the prohibition only applies to the use of genetic information by health plans for underwriting purposes and does not apply to health care providers. If a covered entity, such as an HMO, acts as both a health plan and health care provider, it may use genetic information for purposes of treatment, but may not use such genetic information for underwriting purposes. The Omnibus Rule also clarifies that health plans may not use genetic information for underwriting, even though such a use or disclosure may be considered payment or health care operations.

The Omnibus Rule also requires health plans (except for long-term care plans) that use or disclose PHI for underwriting to include a statement in their NPP that they are prohibited from using or disclosing PHI that is genetic information about an individual for underwriting purposes. Health plans that have already modified and redistributed their NPPs in response to GINA are not required to do so again, provided the changes to the NPP are consistent with the Omnibus Rule.

---

[7] HHS defined "underwriting purposes" as including (1) rules for, or determination of, eligibility for, or determination of, benefits under the plan, coverage or policy; (2) computation of premiums or contribution amounts under the plan, coverage or policy (including discounts, rebates, etc.); (3) application of any pre-existing condition exclusion under the plan, coverage or policy; and (4) other activities related to creating, renewing or replacing a health insurance or health benefit plan. Determination of medical appropriateness is excluded from the definition.

[8] Information on age and sex is also excluded from the definition of "genetic information."

If you would like to receive future ***Health Care Advisories*** electronically, please forward your contact information including e-mail address to **healthcare.advisory@alston.com.** Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Donna P. Bergeson
404.881.7278
donna.bergeson@alston.com

Cathy L. Burgess
202.239.3648
cathy.burgess@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Jennifer L. Butler
202.239.3326
jennifer.butler@alston.com

Brendan Carroll
202.239.3216
brendan.carroll@alston.com

Guillermo Cuevas
202.239.3205
guillermo.cuevas@alston.com

Peter Fise
202.239.3842
peter.fise@alston.com

Joyce Gresko
202.239.3628
joyce.gresko@alston.com

James A. Harvey
404.881.7328
jim.harvey@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Elinor A. Hiller
202.239.3401
elinor.hiller@alston.com

William H. Jordan
404.881.7850
bill.jordan@alston.com

Peter M. Kazon
202.239.3334
peter.kazon@alston.com

David C. Keating
404.881.7355
david.keating@alston.com

Blanche L. Lincoln
202.239.3601
blanche.lincoln@alston.com

Paul G. Martino
202.239.3439
paul.martino@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Kim McWhorter
404.881.4254
kim.mcwhorter@alston.com

Raad S. Missmar
202.239.3034
rudy.missmar@alston.com

William (Mitch) R. Mitchelson, Jr.
404.881.7661
mitch.mitchelson@alston.com

D'Andrea J. Morning
404.881.7538
dandrea.morning@alston.com

Elise N. Paeffgen
202.239.3939
elise.paeffgen@alston.com

Michael H. Park
202.239.3630
michael.park@alston.com

Earl Pomeroy
202.239.3835
earl.pomeroy@alston.com

Steven L. Pottle
404.881.7554
steve.pottle@alston.com

J. Mark Ray
404.881.7739
mark.ray@alston.com

Mark H. Rayder
202.239.3562
mark.rayder@alston.com

Colin Roskey
202.239.3436
colin.roskey@alston.com

Bruce Sarkisian
404.881.4935
bruce.sarkisian@alston.com

Marc J. Scheineson
202.239.3465
marc.scheineson@alston.com

Thomas A. Scully
202.239.3459
thomas.scully@alston.com

Donald E. Segal
202.239.3449
donald.segal@alston.com

Robert G. Siggins
202.239.3836
bob.siggins@alston.com

Carolyn E. Smith
202.239.3566
carolyn.smith@alston.com

Paula M. Stannard
202.239.3626
paula.stannard@alston.com

Trey Stephens
404.881.4392
trey.stephens@alston.com

Robert D. Stone
404.881.7270
rob.stone@alston.com

W.J. "Billy" Tauzin
202.684.9844
billy.tauzin@alston.com

Julie Klish Tibbets
202.239.3444
julie.tibbets@alston.com

Timothy P. Trysla
202.239.3420
tim.trysla@alston.com

Michelle A. Williams
404.881.7594
michelle.williams@alston.com

Marilyn K. Yager
202.239.3341
marilyn.yager@alston.com

Esther Yu
212.210.9568
esther.yu@alston.com

ALSTON & BIRD LLP

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213-576-1100
NEW YORK: 90 Park Avenue ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 275 Middlefield Road ■ Suite 150 ■ Menlo Park, California, USA, 94025-4004 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.756.3300 ■ Fax: 202.756.3333
VENTURA COUNTY: 2801 Townsgate Road ■ Suite 215 ■ Westlake Village, California, USA, 91361 ■ 805.497.9474 ■ Fax: 805.497.8804