McDermott
Will & Emery

OCR Issues Proposed Modifications to HIPAA Privacy and Security Rules to Implement HITECH Act

July 27, 2010

Introduction

On July 14, 2010, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS), issued a proposed rule[1] (Proposed Rule) containing modifications to the privacy standards[2] (Privacy Rule), security standards[3] (Security Rule) and enforcement regulations[4] (Enforcement Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The proposed modifications include changes required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and other changes deemed appropriate by OCR in order to strengthen the privacy and security of health information and to improve the "workability and effectiveness"[5] of the Privacy Rule, Security Rule and Enforcement Rule (collectively, the Administrative Simplification Regulations).

OCR is accepting comments on the Proposed Rule through September 13, 2010. Covered entities, business associates and others affected by the Administrative Simplification Regulations should consider submitting comments to OCR in order to shape the final rule. The Proposed Rule indicates that final amendments to the Administrative Simplification Regulations will be effective 180 days after the publication of a final rule.[6] However, covered entities and business associates that have agreed to comply with HITECH Act requirements or other Administrative Simplification Regulation requirements through business associate agreements will continue to have contractual compliance obligations prior to the effective date.

This *White Paper* addresses the following notable provisions of the Proposed Rule:

- **Part 1:** New privacy and security standards imposed on business associates and their subcontractors
- **Part 2:** Restrictions on marketing involving protected health information[7] (PHI)
- **Part 3**: Restrictions on the sale of PHI
- **Part 4:** Revisions to the requirements for use and disclosure of PHI for research purposes
- **Part 5:** Other significant revisions to the Privacy Rule
- **Part 6:** Revisions to the Enforcement Rule

[1] Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40,867 (proposed July 14, 2010) (to be codified at 45 C.F.R. pts 160 and 164).

[2] 45 C.F.R. pt. 164, subpt. E.

[3] 45 C.F.R. pt. 164, subpt. C.

[4] 71 Fed. Reg. 8,390 (Feb. 16, 2006) (codified at 45 C.F.R. pt. 160, subpts C, D and E); as amended by the interim final rule at 74 Fed. Reg. 56,123 (Oct. 30, 2009) (codified at 45 C.F.R. §§ 160.101, 160.401, 160.404, 160.410, 160.412 and 160.420).

[5] 75 Fed. Reg. at 40,868.

[6] *Id.* at 40,871 (proposed to be codified at 45 C.F.R. § 160.105).

[7] 45 C.F.R. § 160.103.

Part 1: Business Associates and Subcontractors

NEW CATEGORIES OF BUSINESS ASSOCIATES

As required by the HITECH Act,[8] the Proposed Rule would amend the definition of "business associate" to specify that the following additional categories of entities are business associates and, therefore, directly subject to the Administrative Simplification Regulations: organizations that provide data transmission services and that require routine access to such PHI, including health information organizations, regional health information organizations and e-prescribing gateways; and vendors that offer a personal health record to patients on behalf of a covered entity.

APPLICATION OF CERTAIN HIPAA REQUIREMENTS TO BUSINESS ASSOCIATES

The current Security Rule and Privacy Rule impose requirements on covered entities, which include certain health care providers, health plans and health care clearinghouses, and do not regulate business associates directly. Instead, the rules require covered entities to enter into business associate agreements that contractually obligate their business associates to comply with certain business associate agreement requirements. One of the most significant changes made by the HITECH Act was the extension of certain HIPAA and Administrative Simplification Regulation requirements to business associates.

Specifically, the HITECH Act requires business associates to comply with the Security Rule's administrative, physical, and technical safeguards requirements as well as its written compliance policy and documentation requirements.[9] In addition, the HITECH Act requires business associates to comply with the business associate contract requirements of the Privacy Rule.[10] Consequently, effective February 18, 2010, the HITECH Act makes business associates both contractually liable to a covered entity for breach of the business associate agreement with the covered entity and civilly and criminally liable to the government for violations of those Security Rule requirements and the Privacy Rule's business associate agreement requirements. The civil and criminal penalty provisions are discussed further in Part 6 below.

The Proposed Rule would modify the Security Rule and the Privacy Rule to reflect the HITECH Act provisions. In addition, the Proposed Rule includes further amendments to the Privacy Rule and the Security Rule to clarify business associates' compliance obligations and impose additional obligations. For example, the Proposed Rule imposes the Privacy Rule's minimum necessary standard on business associates so that they must limit their requests for and uses and disclosures of PHI to the minimum amount necessary to accomplish the purpose of the use, disclosure or request.[11]

BUSINESS ASSOCIATE AGREEMENTS

The Proposed Rule would modify the current business associate agreement requirements in the Privacy Rule to mandate new contract provisions obligating a business associate to take the following actions:

- To report breaches of unsecured PHI to covered entities in accordance with certain Privacy Rule standards[12]
- To the extent the business associate takes on certain of the covered entity's obligations under the Privacy Rule (*e.g.*, delivery of notices of privacy practices), to comply with the covered entity's obligations[13]

---

[8] HITECH Act § 13,408 (codified at 42 U.S.C. § 17,938).

[9] HITECH Act § 13,401 (codified at 42 U.S.C. § 17,931).

[10] HITECH Act § 13,404 (codified at 42 U.S.C. § 17,934).

[11] *Id.* at 40,919 (proposed to be codified at §164.502(b)).

[12] *Id.* at 40,920 (proposed to be codified at §164.504(e)(2)(ii)(C)).

[13] *Id.* at 40,920 (proposed to be codified at §164.504(e)(2)(ii)(H)).

INCLUSION OF SUBCONTRACTORS AS BUSINESS ASSOCIATES

In addition to the new categories of business associates mandated by the HITECH Act and discussed above, the Proposed Rule adds "subcontractors" (including agents and contractors) of a business associate with access to PHI as a new category of business associate to the extent they are not acting as members of the primary business associate's workforce.[14] This proposed change makes subcontractors subject to HIPAA's civil and criminal penalties in the same manner as primary business associates. Vendors serving the health care industry are likely to object to this proposal on the basis that OCR has exceeded its authority under the HITECH Act, which only made business associates, as defined under the current Administrative Simplification Regulations, subject to certain of the Administrative Simplification Regulations.

DOWNSTREAM BUSINESS ASSOCIATE AGREEMENTS WITH SUBCONTRACTORS

The Proposed Rule does not require a covered entity to enter into a business associate agreement with subcontractor business associates.[15] Instead, as under the current Privacy Rule and Security Rule, the Proposed Rule requires the primary business associates to enter into a downstream business associate agreement with the subcontractor.[16] If a primary business associate knows of a subcontractor business associate's pattern of activity or practice constituting a material breach of a business associate agreement, the primary business associate is required to take reasonable steps to cure the breach or, if such steps were unsuccessful, terminate the contract, if feasible.[17]

TRANSITION PROVISIONS

OCR recognizes that covered entities have existing contracts with business associates and that renegotiation could require significant time and effort. Consequently, the Proposed Rule allows covered entities and business associates to continue operating under business associate agreements that are (1) in effect prior to the date of publication of a final rule in the Federal Register and (2) compliant with the current Administrative Simplification Regulations for up to a maximum of one year and 240 days after the publication date.[18] If the parties to the agreement renew or modify the agreement on or after the date 60 days after the publication date, the Proposed Rule requires the renewal or modification to satisfy the final rule's business associate agreement requirements.[19]

---

[14] 75 Fed. Reg. at 40,913 (proposed to be codified at §160.103).

[15] *Id*. (proposed to be codified at §164.502(e)(1)(i)).

[16] *Id*. (proposed to be codified at §164.502(e)(1)(ii)).

[17] *Id*. at 40,919 (proposed to be codified at §164.504(e)(1)(iii)).

[18] *Id*. at 40,924 (proposed to be codified at §164.532(e)(2)).

[19] *Id*. (proposed to be codified at §164.532(e)(1)).

Part 2: Marketing Restrictions

The current Privacy Rule requires a covered entity to obtain an individual's authorization prior to using or disclosing PHI about the individual for "marketing" purposes unless the use or disclosure satisfies an exception.[20] The Privacy Rule defines marketing as ''to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.''[21]

The current Privacy Rule provides certain exceptions to the marketing authorization requirement, such as for communications in a face-to-face conversation with the individual who is the subject of the PHI or marketing in the form of the provision of a promotional gift of nominal value to the individual.[22] In addition, the current Privacy Rule permits communications without an authorization for a health care provider to provide treatment to the individual and certain health care operations purposes.

In response to concerns that the Privacy Rule permitted too many commercial uses and disclosures of PHI without an individual's authorization under the health care operations exception, the HITECH Act statutorily amended the Privacy Rule, effective February 18, 2010, to provide that certain health care operations communications for which the covered entity receives third-party payment require a marketing authorization.[23]

The Proposed Rule implements the HITECH Act's amendments to the exceptions to the marketing authorization requirements and also proposes various clarifications of the amendments and other changes to the Privacy Rule's marketing standards. The Proposed Rule's marketing provisions are described below.

HEALTH CARE OPERATIONS DISCLOSURES

Consistent with the HITECH Act, the Proposed Rule would require a covered entity to obtain a marketing authorization for the following health care operations communications if the covered entity receives a direct or indirect payment to make such communications:

- To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits[24]

- For case management or care coordination for the individual, contacting of individuals with information about treatment alternatives and related functions, to the extent these activities do not fall within the Privacy Rule's definition of treatment[25]

The Proposed Rule replaces the phrase "direct or indirect payment" in the HITECH Act with "financial remuneration," which is defined as "direct or indirect payment from or on behalf of a third party whose product or service is being described."[26] The definition clarifies that financial remuneration does not include any payment for the treatment of an individual by a health plan or other responsible party.

---

[20] 45 C.F.R. § 164.508(a)(3).

[21] 45 C.F.R. § 164.501.

[22] 45 C.F.R. § 164.501 and 508(a)(3).

[23] HITECH Act § 13,406(a) (codified at 42 U.S.C. § 17,936).

[24] 75 Fed. Reg. at 40,918 (proposed to be codified at 45 C.F.R. § 164.501).

[25] *Id.*

[26] *Id.*

OCR states that financial remuneration does not include other types of remuneration.[27] While the Proposed Rule does not provide a clear standard for distinguishing between financial and nonfinancial remuneration, it appears that the Proposed Rule considers cash and cash equivalents as financial remuneration and in-kind remuneration as nonfinancial remuneration. Accordingly, the Proposed Rule would permit a covered entity to make a mailing for any of the health care operations purposes excluded from the definition of marketing (*e.g.*, providing information about treatment alternatives) in exchange for an in-kind contribution of staff time, envelopes and paper. However, a covered entity should consider anti-kickback and other fraud and abuse laws before implementing such an arrangement since the fraud and abuse laws generally apply more broadly to the conference of any type of benefit, in cash or in kind.

REFILL REMINDERS

The HITECH Act includes an exception to the marketing authorization requirement for health care operations communications for which the covered entity receives payment to permit refill reminders and other communications that describe only a drug or biologic that is currently being prescribed to the individual as long as the payment is reasonable in amount.[28] The Proposed Rule includes the HITECH Act exception for such communications, provided that any financial remuneration received by the covered entity for making the communication is reasonably related to the covered entity's cost of making the communication.[29] OCR requests comment regarding whether communications about drugs that are related to the drug currently being prescribed, such as generic alternatives or new formulations of the drug, should fall within the exception and also requests comment regarding the types and amount of costs that should be allowed under this provision.[30]

TREATMENT COMMUNICATIONS SUBSIDIZED BY THIRD PARTIES

The Proposed Rule proposes to go beyond the marketing restrictions included in the HITECH Act to require a health care provider to provide the following notices to individuals if it will make written treatment communications, without an authorization, in exchange for financial remuneration:

- A statement in its notice of privacy practices that it intends to send such subsidized treatment communications and provide the opportunity for the individual to opt out of receiving such communications.

- A disclosure in the written treatment communication itself that the health care provider is receiving financial remuneration in exchange for the communication and provision of a clear and conspicuous opportunity to the individual to opt out of further such communications. The method for an individual to opt out may not cause the individual to incur an undue burden or incur more than a nominal cost. OCR has requested comments on whether the opt-out should apply to all future subsidized treatment communications or only those dealing with the particular product or service described in the current communication.[31]

Since health care providers may make financially remunerated written treatment communications without an authorization while financially remunerated health care operations communications require an authorization, OCR clarifies that a communication to further the care of a particular individual is a treatment communication while communications in a population-based fashion are health care operations. For example, a blanket mailing to all patients regarding a new service line would be health care operations and require a marketing authorization if it is subsidized by a third party. On the other hand, a provider is making a treatment communication if it sends a pregnant patient a brochure about a birthing center.[32] However, OCR recognizes the practical

---

[27] *Id.* at 40,885.

[28] HITECH Act § 13,406(a)(2)(A) (codified at 42 U.S.C. § 17,936).

[29] *Id.* at 40,918 (to be codified at 45 C.F.R. § 164.501).

[30] *Id.* at 40,885.

[31] *Id.* at 40,923 (to be codified at 45 C.F.R. § 164.514(f)(2)).

[32] *Id.* at 40,886.

difficulty of distinguishing between treatment and health care operations disclosures in certain situations and, therefore, seeks comments on how to address the distinction and related requirements in a final rule.[33]

Part 3: Restrictions on Sale of PHI

PROHIBITION ON SALE OF PHI

The HITECH Act prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of PHI unless the covered entity has obtained an authorization from the individual that states whether the PHI can be further exchanged for remuneration by the entity receiving the PHI unless the disclosure is for:[34]

- Public health activities that section 164.512(b) of the Privacy Rule permits to be disclosed without authorization
- Research purposes permitted by the Privacy Rule, if the price charged for the information reflects the costs of preparation and transmittal of the data[35]
- Treatment of the individual
- The sale, transfer, merger or consolidation of all or part of a covered entity and for related due diligence
- Services rendered by a business associate pursuant to a business associate agreement and at the specific request of the covered entity
- Providing an individual with access to his or her PHI
- Such other purposes as OCR determines to be necessary and appropriate by regulation

The Proposed Rule includes the statutory exceptions and the following additional exceptions and clarifications:

- A covered entity or a business associate may exchange a limited data set for remuneration for public health purposes.[36]
- A covered entity or a business associate may exchange a limited data set for remuneration for research purposes, provided that the price charged for the information reflects the costs of preparation and transmittal of the data.[37]
- A covered entity or a business associate may disclose PHI to obtain payment for health care.[38]
- A covered entity may receive remuneration for a disclosure of PHI required by law.[39]

---

[33] *Id.*

[34] HITECH Act § 13,405(d) (codified at 42 U.S.C. § 17,935).

[35] 75 Fed. Reg. at 40,921 (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(B)); see also discussion of the exception for sale of PHI for research purposes in Part 4 below.

[36] 75 Fed. Reg. at 40,921 (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(A)).

[37] *Id.* (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(B)).

[38] *Id.* (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(C)).

[39] *Id.* (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(G)).

- The Proposed Rule modifies the statutory exception for a payment to a business associate to clarify that the remuneration received by the business associate must be payment for activities performed by the business associate pursuant to a business associate agreement.[40]

- The Proposed Rule clarifies that a covered entity may still charge a reasonable, cost-based fee for multiple requests for an accounting of disclosures in a 12-month period.[41]

- A covered entity may disclose PHI for any other purpose permitted by and in accordance with the applicable requirements of the Privacy Rule if the only remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or is a fee expressly permitted by other law. OCR states that this proposed exception is intended to ensure that the proposed authorization requirement does not deter a covered entity from disclosing PHI for a purpose permitted by the Privacy Rule only because it receives payment of the actual cost of preparing, producing or transmitting the PHI or a fee expressly permitted by law.[42]

AUTHORIZATION STATEMENT

The Proposed Rule requires an authorization for the exchange of PHI for remuneration to include a statement that the covered entity is receiving direct or indirect remuneration in exchange for the PHI.

Part 3: Research Involving PHI

The Privacy Rule generally requires a covered entity to obtain an individual's detailed written authorization[43] before using or disclosing PHI about the individual for research purposes (unless another Privacy Rule disclosure pathway is available). The Privacy Rule requirements are in addition to consent requirements that may apply under the Common Rule[44] or other state and federal privacy and confidentiality laws. Since its inception, the research community has expressed concern that various aspects of the Privacy Rule's authorization requirement have made it more difficult to conduct research, particularly future use research activities. Future use refers to the use of biological materials and/or data originally collected for one purpose for a subsequent purpose, such as research. For example, a health care provider with PHI collected for treatment purposes might want to use the PHI for future research uses not identified at the time of treatment. Similarly, a researcher who collects PHI under an authorization for a primary research study may want to use the PHI to create a repository of data for use in future secondary research studies.

The following subsections describe proposed changes that would facilitate the use and disclosure of PHI for appropriate research activities.

COMPOUND AUTHORIZATION AND ANTI-CONDITIONING RULES

Prior to the Privacy Rule, it was common for a research study's informed consent form to include check-boxes asking the potential subject to indicate whether the individual agreed to participate in certain optional study related activities. Individuals could elect to participate in the main study but decline to participate in the separate, related study activities. In addition, informed consent forms differed widely in the degree to which they described possible future use with specificity. In some cases, individuals were asked to agree upfront to any future use, and in other cases, subjects were given a range of choices from which they could pick and choose. For example, a consent form for a study investigating a new chemotherapy drug might seek consent

[40] *Id.* (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(E)).

[41] *Id.* (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(F)).

[42] *Id.* (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(H)).

[43] The Privacy Rule's authorization requirements are set forth in 45 C.F.R. § 164.508.

[44] 45 C.F.R. § 46.116 and 46.117.

to use any left-over biopsy tissue to look for genetic markers for the cancer type or more generally to store any left-over biopsy tissue for unspecified future use.

The Privacy Rule contains two provisions that generally prohibit the combining into a single informed consent-authorization form permission for the main study (*e.g.*, a clinical trial) with permission for a voluntary, future use study or tissue banking. First, the Privacy Rule prohibits an authorization for the use or disclosure of PHI to be combined with any other document.[45] One exception to this compound authorization ban was that an authorization for the use and disclosure of PHI could be combined with an informed consent form "for the same research study."[46]

Second, the Privacy Rule generally prohibits covered entities from conditioning the provision of treatment (or other services) on an individual's agreement to sign an authorization.[47] One exception to this prohibition is that a covered entity may condition a human subject's receipt of treatment provided during the course of a research study (for example, the experimental chemotherapy agent) on that individual providing an authorization for the use and disclosure of PHI during the course of the research study.[48]

Consequently, covered entities seeking authority for repositories and other future use activities have had to implement a variety of strategies. For example, covered entities have populated their databanks and annotated tissue banks using the limited data set[49] pathway, which restricts the PHI data elements that can be included in a limited data set in ways that are sometimes incompatible with important study objectives. Alternatively, covered entities have presented potential human subjects with multiple forms to cover the main study and then one or more separate, but related, research studies. This approach allows subjects to pick and choose how they participate in research initiatives at the covered entity, but is often confusing and time-consuming for the subjects and may present daunting document retention and management challenges for the covered entity.

The Proposed Rule notes that this approach has been widely criticized and that influential and reputable research advisory bodies have encouraged OCR to reconsider the research authorization requirements.[50] In light of these logistical hurdles and the research community's continuing sustained concern that this prohibition complicates research with little benefit to protecting confidentiality, OCR is proposing to amend the research authorization requirements to "allow a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities."[51] Specifically, the Proposed Rule provides that an authorization for a research study may be combined with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research.

The Proposed Rule provides an illustrative list of possible approaches to effectively designing such compound forms but requests comments on "additional methods that would clearly differentiate to the individual the conditioned and unconditioned research activities on the compound authorization."[52]

---

[45] *Id*. at 164.508(b)(3).

[46] *Id*. at 164.508(b)(3)(i).

[47] *Id*. at 164.508(b)(4).

[48] *Id*. at 164.508(b)(4)(i).

[49] *Id*. at 164.514(e).

[50] 75 Fed. Reg. at 40892-93 (see, for example, the Secretary's Advisory Committee for Human Research Protections in 2004, Recommendation V, submitted in a letter to the Secretary of HHS, available at http://www.hhs.gov/ohrp/sachrp/hipaalettertosecy090104.html).

[51] *Id*. at 40,893.

[52] *Id*. at 40,893.

AUTHORIZATION SPECIFICITY REQUIREMENT

The Privacy Rule requires certain elements for a valid authorization, including that the authorization describe with specificity the uses and disclosures being authorized.[53] The specificity requirement has posed a problem for future use because it typically requires data and biological materials to be warehoused long-term to support any number of possible future uses and it is often not feasible to specify the nature of such uses at the time that the data and biological materials are collected. In addition, the specificity requirement differs from the long-standing Common Rule approach that allowed for greater flexibility, subject to institutional review board (IRB) approval, for obtaining informed consent for future use.

In light of these concerns, OCR indicates in the Proposed Rule that it is considering and seeking comments on amending "its interpretation" of the specificity requirement as applied to research. The OCR did not propose new language at this time but instead seeks comments on a number of proposed approaches to permitting compound authorizations for unspecified future use, including the following:[54]

- "[A]n authorization for uses and disclosures of PHI for future research purposes to the extent such proposes are adequately described in the authorization such that it would be reasonable for the individual to expect that the PHI could be used or disclosed for such future research"

- "[A]n authorization for future research only to the extent the description of the future research included certain elements or statements specified by the Privacy Rule, and if so, what should those be"

- The option described in the first bullet "as a general rule but require certain disclosure statements on the authorization in cases where the future research may encompass certain types of sensitive research activities, such as research involving genetic analyses or mental health research, that may alter an individual's willingness to participate in the research"

OCR is also interested in receiving comments on how subjects might revoke their permission to use and disclose PHI for future uses.[55] OCR intends to consider comments on these issues and to coordinate its efforts with the Office of Human Research Protections and the Food and Drug Administration in an effort to harmonize agency approaches to future use questions. Any changes would be included in the Final Rule.

SALE OF PHI FOR RESEARCH PURPOSES

As noted in Section 3 above, the HITECH Act prohibits a covered entity from receiving remuneration in exchange for the disclosure of PHI unless the covered entity has obtained an authorization or an exception applies.[56] One exception in the Act is for disclosure for research purposes permitted by the Privacy Rule, but only if the price charged for the information reflects the costs of preparation and transmittal of the data.[57] The HITECH Act also instructed OCR to consider the impact of this cost-based payment condition on the exception for research when developing implementing regulations. The Proposed Regulations would revise the language of the research exception specifically to clarify that the cost-based payment condition applies to the exchange of a limited data set for remuneration for research purposes.[58] This clarification reinforces a concern about the feasibility of data and tissue research repository collaborations in which the parties may share the valuable rights of access to one another's information in return for contributions of capital, data and tissue to the repository. The possibility that such access rights will be considered remuneration above costs incurred to disclose PHI in connection with the creation and operation of the repository, and thereby trigger the need for an authorization, may impede collaborations among providers to create robust repositories that will

[53] 45 C.F.R. § 164.508(c)(1)(i).

[54] *Id.* at 40,894.

[55] *Id.*

[56] HITECH Act §13,405(d) (codified at 42 U.S.C. § 17,935).

[57] HITECH Act §13,405(d)(2)(B) (codified at 42 U.S.C. § 17,935).

[58] *Id.* (proposed to be codified at 45 C.F.R. § 164.508(a)(4)(ii)(B)); See also the discussion of the exception for sale of PHI for research purposes in Part 4 below.

enhance their quality measurement and reporting capabilities and fuel translational research and the personalized medicine movement. Arguably, such an interpretation would limit the flexibility the current Privacy Rule affords for use of data and tissue repositories for research without an authorization. Whether such a result was intended or should be avoided is worthy of further consideration by OCR in the development of the final regulations.

Part 4: Other Proposed Revisions to the Privacy Rule

This section addresses proposed changes and guidance to the Privacy Rule's standards regarding minimum necessary PHI, fundraising communications, an individual's right to request restrictions on the disclosure of PHI, notices of privacy practices, and access to PHI in a designated record set.

MINIMUM NECESSARY STANDARD

For most uses and disclosures of PHI for non-treatment purposes, the Privacy Rule requires covered entities to limit requests for and uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose of the request, use or disclosure.[59] The HITECH Act requires OCR to issue guidance on what constitutes the minimum necessary amount of PHI to accomplish the intended purpose of a use, disclosure or request.[60] The Proposed Rule solicits comments on the aspects of the minimum necessary standard for which covered entities and business associates seek guidance.[61] OCR proposes to leave the current regulatory text unchanged, however, as the guidance they will issue on minimum necessary will obviate the need to make any changes to the current language.[62]

In the interim, the HITECH Act specifies that a covered entity will be in compliance with the minimum necessary standard as long as it limits PHI, to the extent practicable, to either (a) the equivalent of a limited data set, or (b) if a covered entity decides that the limited data set does not meet the needs of the particular use, disclosure or request, it may go beyond the limited data set if it does so according to its then-compliant minimum necessary policies and procedures. This temporary standard sunsets as soon as the guidance regarding minimum necessary is issued.[63]

FUNDRAISING DISCLOSURES

Currently, the Privacy Rule permits a covered entity to use or disclose for fundraising purposes an individual's demographic information and the dates health care was provided to that individual.[64] No authorization is required to make such uses and disclosures, but, as discussed in the following subsection, the covered entity's notice of privacy practices must inform individuals that the covered entity may contact them to raise funds. Also, fundraising materials must describe how the individual may opt out, and the covered entity must make reasonable efforts to ensure that individuals who opt out are not sent future fundraising communications.

---

[59] 45 C.F.R. § 164.502(b)(1).

[60] HITECH Act § 13,405(b)(1)(B) (to be codified at 45 C.F.R. pts. 160, 164).

[61] 75 Fed. Reg. at 40,896.

[62] *Id*.

[63] HITECH Act § 13,405(b)(1)(C) (codified at 42 U.S.C. § 17,935).

[64] 45 C.F.R. § 514(f).

The HITECH Act requires a covered entity to provide the recipient of fundraising information a *clear and conspicuous* opportunity for the individual to opt out of receiving any further fundraising communications.[65] The Proposed Rule would implement this change. The Proposed Rule would make the following additional changes to the fundraising requirements deemed advisable by OCR:

- The method for opting out may not cause the individual to incur an undue burden or more than nominal cost.
- The covered entity must not condition treatment or payment on an individual's choice with respect to receiving fundraising communications.
- The covered entity must ensure that no fundraising communications are sent to an individual who has opted out, rather than only making "reasonable efforts" to do so.

The Proposed Rule requests comments on the following issues related to fundraising communications:

- To what fundraising communications an opt-out requirement should apply
- How an individual could choose to opt back in to receiving such communications
- Whether the Privacy Rule should allow additional categories of PHI to be used or disclosed for fundraising, and if so, what those categories should be
- The adequacy of the minimum necessary standard to appropriately limit the amount of PHI that may be used or disclosed for fundraising purposes
- Whether the current limitations to use of PHI for fundraising communications remain unchanged *(e.g.*, dates of treatment, demographic info)
- Whether an opt-out should be offered before the first fundraising communication, and the process for such an opt-out

Tax-exempt covered entities should consider submitting comments on these important issues. In particular, limitations on the categories of PHI that may be used for fundraising purposes have interfered with targeted fundraising for development initiatives that are more likely to appeal to patients (or their families) with particular conditions or disease states. For example, the current fundraising requirements do not permit a tax-exempt hospital from using cancer diagnosis information to send a targeted fundraising appeal for a new cancer center to cancer patients and their families.

PATIENT RIGHT TO REQUEST RESTRICTIONS ON DISCLOSURES OF PHI TO HEALTH PLANS

The current Privacy Rule requires a covered entity to permit individuals to request that the covered entity restrict uses or disclosures of PHI for treatment, payment and health care operations purposes, as well as for disclosures to family members and others involved in the patient's care.[66] The covered entity is not required to agree to a requested restriction.

The HITECH Act[67] amends the right to request additional restrictions to require (unless otherwise required by law) a covered entity to agree to a requested restriction if the request regards disclosures of PHI to a health plan for the purpose of carrying out payment or health care operations and the restriction applies to PHI that pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full. The Proposed Rule would implement the HITECH Act

[65] HITECH Act § 13,406(b) (codified at 42 U.S.C. § 17,936).

[66] 45 C.F.R. § 164.522(a).

[67] HITECH Act 13405(a) (codified at 42 U.S.C. §17,935).

requirement.[68] The Proposed Rule clarifies that where a restriction has been placed on a disclosure to a health plan, the covered entity is also prohibited from making such disclosure to a business associate of the health plan.

The Proposed Rule provides that an individual may determine for which health care items or services the individual wishes to pay out of pocket and restrict disclosures to a health plan. OCR notes, for example, "an individual who regularly visits the same provider for the treatment of both asthma and diabetes must be able to request, and have the provider honor, a restriction on the disclosure of diabetes-related treatment to the health plan as long as the individual pays out of pocket for this care. The provider cannot require that the individual apply the restriction to all care given by the provider and, as a result, cannot require the individual to pay out of pocket for both the diabetes and asthma-related care in order to have the restriction on the diabetes care honored."[69]

The Proposed Rule provides that the requirement that the covered entity be paid in full for the health care item or service for which the individual requests a restriction is not limited to situations where the patient is the person paying the covered entity. It also applies when a family member or another person pays for the treatment.

OCR requests comments on the types of interactions between individuals and covered entities that would make requesting or implementing a restriction more difficult.

DOWNSTREAM HEALTH CARE PROVIDERS

OCR requests comments on the obligation of health care providers that know of a restriction to inform other health care providers downstream of such restriction.[70] OCR is interested in whether a restriction placed upon certain PHI should apply to, and the feasibility of it continuing to attach to, such information as it moves downstream, or if the restriction should no longer apply until the individual visits a new provider for treatment or services, requests a restriction, and pays out of pocket for the treatment. In conjunction with this request, OCR seeks comments regarding the extent to which technical capabilities exist that would facilitate notification among providers of restrictions on the disclosure of PHI, how widely these technologies are currently utilized, and any limitations in the technology that would require additional manual or other procedures to provide notification of restrictions. In particular, OCR specifically requests suggestions of methods through which a provider, using an automated electronic prescribing tool, could alert a pharmacy that the patient may wish to request that a restriction be placed on the disclosure of PHI to the health plan and that the patient intends to pay out of pocket for the prescription.

COST-SHARING AND MANAGED CARE ISSUES

OCR emphasizes that when a patient requests a restriction of information to a health plan and pays out of pocket, that patient should not expect that this payment will count towards the out of pocket threshold with respect to his or her health plan benefits[71] because the health plan will be unaware of any payment for treatment or services.

OCR requests commentary on how this provision will function with respect to HMOs. Under most current HMO contracts with providers, an individual could not pay the provider for the treatment or service received, and individuals who belong to an HMO may be obligated to use an out-of-network provider if they wish to ensure that certain PHI is not disclosed to the HMO.[72]

PERMITTED DISCLOSURE FOR UNRESOLVED NON-PAYMENT

The Proposed Rule advises that if an individual fails to honor the promise to make the out of pocket payment for a health care item or service that entitles him or her to request the additional restriction (*e.g.*, the individual's check bounces), the covered

---

[68] 75 Fed. Reg. at 40,923 (proposed to be codified at 45 C.F.R. § 164.522).

[69] 75 Fed. Reg. at 40,899 (proposed to be codified at 45 C.F.R. § 164.522(a)(1)).

[70] *Id.*

[71] 75 Fed. Reg. at 40,900.

[72] *Id.*

entity may then submit the information to the health plan for payment.[73] OCR does make clear, however, that covered entities are expected to attempt to resolve the payment issue with the patient prior to sending the PHI to the health plan. Providers may attempt resolution by notifying the individual that his or her payment did not go through and give the individual an opportunity to submit payment. OCR requests comments with regard to the extent to which covered entities must make reasonable efforts to secure payment from the individual prior to submitting PHI to the health plan for payment.[74]

NOTICE OF PRIVACY PRACTICES

The Privacy Rule currently requires a covered entity's notice of privacy practices (NPP) to include a statement that any uses and disclosures other than those permitted by the Privacy Rule will be made only with the written authorization of the individual.[75] The Proposed Rule would make several changes to the Privacy Rule's NPP requirements to assure that individuals are aware of the types of uses and disclosures that require an authorization or the right to opt-out:

- As discussed in Part 2 regarding new restrictions on marketing communication, if a health care provider intends to send written treatment communications to an individual concerning treatment alternatives or other health-related products or services in exchange for financial remuneration, the NPP must include a statement informing individuals of the practice. The NPP must also inform the individual that he or she has the opportunity to opt out of receiving such communications.[76]

- As described above, the Proposed Rule would require the NPP to include a notice that the covered entity intends to send fundraising communications and to inform the individual that he or she has the right to opt out of such communications.[77]

- The NPP must include a statement that describes the new requirement that a covered entity must accommodate a request to restrict disclosures of PHI pertaining solely to health care for which the individual or a person other than a health plan has paid in full.[78]

OCR requests comments on whether to require an NPP to include a statement regarding notification requirements following a security breach of unsecured PHI and the method of informing individuals of changes to an NPP that would not unduly burden health plans.

ACCESS

The Privacy Rule currently provides a right for individuals to review or obtain copies of their PHI, with limited exceptions, to the extent such information is maintained in the designated record sets of a covered entity.[79] Designated record sets are medical and billing records of a health care provider, the enrollment, payment, claims adjudication and case or medical management records of a health plan, or other records used by a covered entity to make decisions about an individual.[80] The HITECH Act expands the right of access by requiring a covered entity that maintains an electronic health record (EHR) to provide the individual with a copy of such information in an electronic format.[81] The individual may direct the covered entity to transmit such copy directly to

---

[73] *Id.*

[74] *Id.*

[75] 45 C.F.R. 164.520(b)(1)(ii)(E).

[76] 75 Fed. Reg. at 40,923 (proposed to be codified at 45 C.F.R. § 164.520(b)(1)(iii)(A)); see also Part 2 of this *White Paper* infra.

[77] Id. (proposed to be codified at 45 C.F.R. § 164.520(b)(1)(iii)(B)).

[78] 75 Fed. Reg. at 40,923 (proposed to be codified at 45 C.F.R. § 164.522(a)(1)(vi)).

[79] 45 C.F.R. § 164.524.

[80] 45 C.F.R. § 164.501.

[81] HITECH Act § 13,405(e) (codified at 42 U.S.C. § 17,935).

the individual's designee, provided that any such choice is clear, conspicuous and specific. The HITECH Act also provides that any fee imposed by the covered entity for providing such an electronic copy shall not be greater than the entity's labor costs in responding to the request for the copy.[82]

The HITECH Act only addresses PHI in EHRs. However, OCR notes that incorporating these new provisions in such a limited manner in the Privacy Rule could result in a complex set of disparate requirements for access to PHI in EHRs and other types of electronic record systems. Therefore, the Proposed Rule includes a number of changes to an individual's right to access PHI to promote a more uniform right to access all PHI maintained in one or more designated record sets electronically, regardless of whether the designated record set is an electronic health record.

FORM OR FORMAT REQUESTED

Under the Proposed Rule, if the PHI requested 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 it is readily producible, or if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

ACCESS BY DESIGNEES

The Privacy Rule currently requires a covered entity to provide the access requested in a timely manner, which includes arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of PHI at the individual's request.[83] Under the Proposed Rule, a covered entity must transmit the copy of PHI directly to another person designated by the individual, whether or not the PHI is in electronic or paper form, if clearly, conspicuously and specifically requested by the individual.[84]

TIMELINESS

Under the current Privacy Rule, a request for access must be approved or denied, and if approved, access to or a copy of the information provided, within 30 days of the request. In cases in which the records requested are only accessible from an off-site location, the covered entity has an additional 30 days to respond to the request.[85] In extenuating circumstances in which access cannot be provided within these timeframes, the covered entity may have a one-time 30-day extension if the individual is notified of the need for the extension within the original timeframes.[86]

OCR requests comments with regard to the timeliness requirements for provision of access.[87] OCR desires to address the expectation that, with the advance of electronic health records, there is capacity to provide individuals with almost instantaneous electronic access to the PHI in those records through personal health records or similar electronic means.

---

[82] *Id.*

[83] 45 C.F.R. § 164.524(c)(3).

[84] 75 Fed. Reg. at 40,902 (proposed to be codified at 45 C.F.R. § 164.524(c)(3)); see also HITECH Act § 13405(e)(1) (codified at 42 U.S.C. § 17,935).

[85] 45 C.F.R. § 164.524(b).

[86] *Id.*

[87] 75 Fed. Reg. at 40,903.

OCR also requests comments on the following topics related to timeliness for provision of access:[88]

- Whether there is an appropriate, common timeliness standard for the provision of access by covered entities with electronic designated record sets generally. OCR would like to examine aspects of existing systems that would create efficiencies in processing of requests for electronic information, as well as those aspects of electronic systems that would provide little change from the time required for processing a paper record.

- Whether the current standard could be altered for all systems, paper and electronic, such that all requests for access should be responded to without unreasonable delay and not later than 30 days.

- Whether, contrary to OCR's assumption, a variety of timeliness standards based on the type of electronic designated record set is the preferred approach and, if so, how OCR should operationalize such an approach.

- How much time is necessary for covered entities to review access requests and make necessary determinations, such as whether the granting of access would endanger the individual or other persons. OCR wants to better understand how the time needed for these reviews relates to the overall time needed to provide the individual with access.

- Whether the provision which allows a covered entity an additional 30 days to provide access to the individual if the PHI is maintained off-site should be eliminated altogether for both paper and electronic records, or at least for PHI maintained or archived electronically because the physical location of electronic data storage is not relevant to its accessibility.

Part 6: Modifications to the Enforcement Rule

The HITECH Act significantly modified the categories of HIPAA violations, the range of civil money penalty amounts and the available defenses to a HIPAA action. These HITECH Act provisions became effective for covered entities on February 18, 2009, and made business associates directly subject to HIPAA's enforcement scheme for the first time beginning February 18, 2010.[89]

On October 30, 2009, OCR issued an interim final rule to implement the HITECH Act's amendments to the enforcement provisions of the current Privacy Rule.[90] The Interim Final Enforcement Rule became effective November 30, 2009.[91] The Proposed Rule proposes a number of significant changes to the Enforcement Rule's provisions concerning compliance and investigations[92] and the imposition of civil money penalties[93] to implement HITECH Act provisions that become effective in 2010 and 2011.

MANDATORY INVESTIGATIONS VERSUS USE OF "INFORMAL MEANS"

Currently, the Enforcement Rule permits, but does not require, OCR to investigate HIPAA violation complaints. The Proposed Regulation would amend the Enforcement Rule, consistent with the HITECH Act, to require the OCR to investigate any complaint when a preliminary review of the facts indicates a possible violation due to willful neglect. The Enforcement Rule defines willful neglect to mean "conscious, intentional failure or reckless indifference to the obligation to comply with the

---

[88] Id.

[89] HITECH Act § 13,423 (codified at 42 U.S.C. § 17,953); see also 75 Fed. Reg. at 40,871 (explaining that one year after the date of enactment is February 18, 2010).

[90] 74 Fed. Reg. 56,123 (codified at 45 C.F.R. §§ 160.101, 160.401, 160.404, 160.410, 160.412 and 160.420).

[91] For more information on the Interim Final Enforcement Rule, see our *On* the Subject titled, "HHS Issues Interim Final Rule Conforming HIPAA Civil Money Penalties to HITECH Act Requirements," available at http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/ae68626d-301b-4aa7-9a20-911cbe1b1f4a.cfm.

[92] 45 C.F.R. § 160.300 *et seq*.

[93] 45 C.F.R. § 160.400 *et seq*.

administrative simplification provision violated."[94] The Proposed Rule would maintain OCR's discretion to decline to investigate a complaint where a preliminary investigation does not indicate that the alleged violation is due to willful neglect.[95] However, as a practical matter, the proposed amendment would not alter OCR's current policy of investigating any alleged violation where a preliminary review suggests a potential HIPAA violation.

The Interim Final Enforcement Rule also currently requires OCR to attempt to resolve noncompliance through "informal means." In order to permit OCR to impose a civil money penalty for violations due to willful neglect as required by the HITECH Act, however, the Proposed Rule proposes to amend the Enforcement Rule by *permitting, but not requiring*, OCR to use "informal means" to resolve noncompliance.[96]

TIERED PENALTY SCHEME

The HITECH Act and the Interim Final Enforcement Rule implemented a new tiered civil money penalty structure based on the following culpability levels: (1) the entity did not know (and, by exercising reasonable diligence, would not have known) that it violated the applicable provision; (2) the violation is due to reasonable cause and not to willful neglect; (3) the violation is due to willful neglect and was corrected during the 30-day period beginning on the first date the entity knew, or, by exercising reasonable diligence, would have known that the violation occurred; or (4) the violation is due to willful neglect and was not corrected during the 30-day period beginning on the first date the entity knew, or, by exercising reasonable diligence, would have known that the violation occurred. The Proposed Rule would further clarify the culpability levels by amending the definition of "reasonable cause." Under the proposed definition, "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."[97]

The Proposed Rule also attempts to provide guidance with respect to how OCR intends to apply the terms "reasonable cause," "reasonable diligence," and "willful neglect" used in the tiered penalty scheme by providing hypothetical examples for each tier.[98] For example, the OCR stated that the failure to develop or implement compliant HIPAA policies and procedures "demonstrate[s] either conscious intent or reckless disregard with respect to . . . compliance obligations," and may be the basis for a finding of a violation due to willful neglect.[99] The OCR also notes that a covered entity's or a business associate's correction of a violation due to willful neglect will not prevent the imposition of a civil money penalty, but may prevent the violation from falling into the highest culpability level. Accordingly, covered entities and business associates should assure that current policies appropriately implement current requirements and be prepared to amend the current policies once the OCR issues a final rule.

DETERMINING THE AMOUNT OF A CIVIL MONEY PENALTY WITHIN TIERED PENALTY RANGES

The Enforcement Rule sets forth the factors to be considered by OCR when determining a civil money penalty for a violation within the approved penalty range for the culpability tier.[100] The HITECH Act does not add or delete factors, but requires OCR to base its penalty determination "on the nature and extent of the violation and the nature and extent of the harm resulting from such violation."[101] Accordingly, the Proposed Rule proposes to amend the factors to clarify that the OCR must consider the nature and

---

[94] 45 C.F.R. § 160.401.

[95] 45 C.F.R. § 160.306(c)(2).

[96] 75 Fed. Reg. at 40,877 (proposed to be codified at § 160.312(a)(1)).

[97] 45 C.F.R. § 160.401.

[98] 75 Fed. Reg. 40,878–79.

[99] 75 Fed. Reg. 40,879.

[100] 45 C.F.R. § 160.408.

[101] HITECH Act § 13401(d) (adding new subsection (c) to 42 U.S.C. 1320d–5).

extent of the violation and the nature and extent of the harm resulting from the violation.[102] The Proposed Rule would also permit OCR, when taking into account the nature and the extent of a violation, to consider the number of individuals affected and the time period during which the violation occurred, and, when taking into account the nature and the extent of the harm resulting from a violation, to consider the physical, financial or reputational harm and whether the violation hindered an individual's ability to obtain health care.

AFFIRMATIVE DEFENSES

The Proposed Rule proposes to revise the Enforcement Rule's affirmative defenses to accommodate a revision to the HIPAA criminal penalties provision, which becomes effective on February 18, 2011. HIPAA currently provides that a civil money penalty may not be imposed with respect to an act "*if the act constitutes an offense punishable*" under the HIPAA criminal penalties provisions. Effective February 18, 2011, the HITECH Act replaces the italicized phrase with "*if a penalty has been imposed*" for the act. Accordingly, the Proposed Rule revises the Enforcement Rule's affirmative defenses as follows:

- For violations occurring after February 18, 2009, but prior to February 18, 2011, the OCR may not impose a civil money penalty on a covered entity or business associate if the covered entity or business associate establishes that the violation *is an offense punishable under* the HIPAA criminal penalties provisions.

- For violations occurring on or after February 18, 2011, the OCR may not impose a civil money penalty on a covered entity or business associate if the covered entity or business associate establishes that a penalty *has been imposed* under the HIPAA criminal penalties provisions.

HIPAA COMPLIANCE REVIEWS

The Enforcement Rule authorizes the OCR to conduct discretionary compliance reviews of covered entities and business associates outside of the HIPAA complaint process.[103] The Proposed Rule would amend the provision to require the OCR to conduct compliance reviews to determine whether a covered entity or business associate is complying with the applicable administrative simplification provision when a preliminary review indicates a potential violation due to willful neglect. The Proposed Rule maintains the OCR's discretion where a preliminary review does not indicate willful neglect.

APPLICATION OF ENFORCEMENT RULE TO BUSINESS ASSOCIATES

As required by the HITECH Act, the Proposed Rule makes the Enforcement Rule directly applicable to business associates rather than only indirectly applicable through business associate agreements between covered entities and business associates. To account for the direct application of the regulations to business associates, the Proposed Rule revises a number of sections of the Enforcement Rule by adding the term "business associate" where appropriate.[104]

VICARIOUS LIABILITY FOR VIOLATION BY WORKFORCE MEMBERS OF AGENTS

Under the current Enforcement Rule, a covered entity is liable for the violations of its workforce members and other agents in accordance with the federal common law of agency,[105] except where the agent is a business associate, the relevant business associate agreement requirements have been met, the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and the covered entity did not fail to act as required by the Privacy Rule or Security Rule with respect to such violations. The Proposed Rule would remove this exception so that the covered entity remains liable for the acts of its agents which are business associates, regardless of whether the covered entity has a compliant business associate agreement in

---

[102] 75 Fed. Reg. 40,880 (proposed to be codified at § 160.408).

[103] 45 C.F.R. § 160.308.

[104] 75 Fed. Reg. 40,875 (proposing to insert term "business associate" following references to "covered entity" at 45 C.F.R. §§ 160.300; 160.304; 160.306(a) and (c); 160.308; 160.310; 160.312; 160.316; 160.401; 160.402; 160.404(b); 160.406; 160.408(c) and (d); and 160.410(a) and (c)).

[105] 45 C.F.R. § 160.402(c).

place. The Proposed Rule also provides for civil money penalty liability against a business associate for the acts of its workforce members and downstream business associates that are agents acting within the common law scope of agency.

If finalized, this change would significantly heighten the risks of failing to conduct reasonable due diligence on the privacy and security practices of prospective business associates and subcontractors and of inadequate monitoring of retained business associates and subcontractors. Covered entities and business associates should consult with their health information technology team and data privacy and security counsel to determine a prudent level of due diligence on vendors before outsourcing activities involving the use and disclosure of PHI.

A determination of whether a business associate or subcontractor is an agent for whom the principal is vicariously liable under the Proposed Rule or is instead an independent contractor requires a case-by-case inquiry based on the facts of the relationship, including the covered entity's level of control over the vendor's conduct. To avoid vicarious liability, a covered entity or business associate principal needs to walk a narrow line between not having enough control to transform a vendor into an agent and sufficient oversight to be aware of the vendor's noncompliant activities. The right balance can be addressed by conducting a vendor privacy and security assessment in advance and by carefully structuring business associate agreements and downstream subcontractor agreements to provide an appropriate level of oversight.

For more information, please contact your regular McDermott lawyer, or:

Daniel F. Gottlieb: +1 312 984 6471 dgottlieb@mwe.com
Bernadette M. Broccolo: +1 312 984 6911 bbroccolo@mwe.com
Jennifer S. Geetter: +1 202 756 8205 jgeetter@mwe.com
Jerry Tichner: +1 617 535 4094 jtichner@mwe.com
Jeanna Palmer Gunville: +1 312 984 7620 jgunville@mwe.com
Sarah Nelson: + 1 310 551 9324 snelson@mwe.com
Edward G. Zacharias: +1 617 535 4018 ezacharias@mwe.com
Stephen W. Bernstein: +1 617 535 4062 sbernstein@mwe.com

For more information about McDermott Will & Emery visit www.mwe.com