McDermott
Will & Emery

OCR Issues Final Modifications to the HIPAA Privacy, Security, Breach Notification and Enforcement Rules to Implement the HITECH Act

February 20, 2013

On January 25, 2013, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) published a final rule (Final Rule) containing modifications to the privacy standards (Privacy Rule), security standards (Security Rule), interim final security breach notification standards (Breach Notification Rule) and enforcement regulations (Enforcement Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The final modifications include changes required by the HITECH Act and other changes deemed appropriate by OCR in order to strengthen the privacy and security of health information.

The Final Rule contains a number of provisions that will affect a broad range of HIPAA covered entities (which include certain health care providers, health plans and health care clearinghouses) and the vendors that provide services to them involving protected health information (PHI) (*i.e.*, generally, individually identifiable health information other than employment records and certain education records):

- As required by the HITECH Act, business associates are directly liable for civil money penalties (CMPs) and criminal penalties for violations of the Privacy Rule and Security Rule.

- The definition of business associate is expanded to include a subcontractor of a business associate so that subcontractors of a business associate are also liable for violations of the Privacy Rule and Security Rule.

- The definition of a breach of unsecured PHI is revised to make it more difficult for a covered entity or business associate to avoid reporting an unauthorized use or disclosure of PHI to the affected individuals and OCR.

- Except in limited cases, a covered entity may not receive cash or other financial remuneration for marketing communications made for a third party's products or services.

- Certain restrictions on the use of compound authorizations in connection with research studies purposes were changed in a way that will facilitate certain secondary uses of PHI for research purposes. The Final Rule does not change the requirement that a valid authorization must include a description of each "purpose" of a requested use and/or disclosure of PHI. In the Final Rule preamble, however, OCR states that it will no longer interpret the "purpose" requirement to mean that an authorization used in connection with a research study must identify a specific study for which the PHI will be used.

Notably, the Final Rule does not address the accounting for disclosures requirement in Section 13405 of the HITECH Act. OCR advises that it will be the subject of a future rulemaking.

Regulatory History

The Privacy Rule, Security Rule and Enforcement Rule implement certain of the administrative simplification provisions of HIPAA. On February 17, 2009, Congress adopted the HITECH Act, which requires certain modifications to those rules and imposes new requirements for notification of breaches of unsecured PHI.[1] OCR published the Breach Notification Rule on August 24, 2009 to implement the breach notification requirements effective September 23, 2009.[2] In addition, to conform the Enforcement Rule to the HITECH Act's stepped up enforcement provisions, OCR published an interim final enforcement rule on October 30, 2009 (Interim Enforcement Rule).[3]

On July 14, 2010, OCR published a notice of proposed rule making to implement most of the HITECH Act's privacy, security and enforcement provisions which were not already implemented through the Breach Notification Rule and the Interim

[1] See our *White Paper* regarding the HITECH Act, "Economic Stimulus Package: Policy Implications of the Financial Incentives to Promote Health IT and New Privacy and Security Protections," available at www.mwe.com/info/news/wp0209e.pdf.
[2] See our *White Paper* regarding the Breach Notification Rule, "Regulatory Update: HITECH's HHS and FTC Security Breach Requirements," available at www.mwe.com/info/news/wp0809b.pdf.
[3] See our *On the Subject* publication, "HHS Issues Interim Final Rule Conforming HIPAA Civil Money Penalties to HITECH Act Requirements," available at www.mwe.com/publications/uniEntity.aspx?xpST=PublicationDetail&pub=5322&PublicationTypes=d9093adb-e95d-4f19-819a-f0bb5170ab6d.

Enforcement Rule and to make other changes that OCR deemed appropriate. On May 31, 2011, OCR published a notice of proposed rule making to implement the HITECH Act's accounting of disclosures requirement.[4]

The following chart summarizes the following key provisions of the Final Rule:

- New privacy and security standards imposed on business associates and their subcontractors
- Revision to the definition of "breach"
- Restrictions on marketing involving PHI
- Restrictions on the sale of PHI
- Restrictions on the use and disclosure of PHI for fundraising
- Revisions to the authorization requirements for research and other secondary uses of PHI
- Revisions to the Enforcement Rule

[4] See our *White Paper* regarding the proposed modifications to the Privacy Rule's accounting of disclosures standard, "OCR Issues Proposed Modifications to HIPAA Privacy and Security Rules to Implement HITECH Act," available at www.mwe.com/info/news/wp0710c.pdf.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
Business Associate and Subcontractor Provisions			
Who is a Business Associate? **(45 CFR § 160.103)**	The Privacy Rule's definition of business associate includes two categories of business associates. ***Category 1*** Business associate means a person who, on behalf of a covered entity or organized health care arrangement in which the covered entity participates (but other than in the capacity of a member of the workforce of the covered entity or arrangement), performs or assists in the performance of any function or activity regulated by the Privacy Rule. ***Category 2*** Business associate also means a person (other than in the capacity of a member of a covered entity's workforce) who, with respect to a covered entity, provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.	Like the current Privacy Rule, the Final Rule maintains two categories within the business associate definition. However, the Final Rule revises the first category of the definition of business associate as described below and also specifically identifies certain types of persons in the definition. ***Category 1*** The Final Rule revises the first category of the definition of business associate to mean a person who on behalf of a covered entity or of an organized health care arrangement in which the covered entity participates (other than in the capacity of a member of the workforce of such covered entity or arrangement) creates, receives, maintains or transmits PHI for a function or activity regulated by the Privacy Rule. ***Category 2*** Category 2 of the definition is substantially the same as the definition in the current Privacy Rule. ***Subcontractors and Other Specific Inclusions*** The Final Rule specifically includes the following persons within the definition of a business associate: ▪ Any subcontractor of a business associate that creates, receives, maintains or transmits PHI on behalf of a business	A person that receives PHI from a covered entity or a business associate, but has previously concluded that he/she or it is not a business associate should revisit that conclusion. For example, OCR makes clear in the Final Rule preamble, and through the modification of the definition, that entities that "maintain" PHI on behalf of a covered entity (such as data storage vendors and cloud service vendors) are business associates.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		associate ▪ Health information organizations (such as a regional health information exchange) ▪ E-prescribing gateways ▪ Other persons that provide data transmission services with respect to PHI to a covered entity and that require access on a routine basis to such PHI ▪ Vendors that offer personal health records to one or more individuals on behalf of a covered entity	
Applicability of Privacy Rule and Security Rule to Business Associates **(45 CFR § 164.104)**	The current Privacy Rule and Security Rule directly apply only to covered entities (*i.e.*, health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a covered transaction). Business associates and their subcontractors are only indirectly subject to the Privacy Rule and Security Rule contractually through business associate agreements with covered entities and downstream business associate agreements between business associates and their subcontractors.	As required by the HITECH Act, the Final Rule requires business associates to comply with the Privacy Rule and the Security Rule. A business associate is potentially subject to CMPs and criminal penalties for a violation of the Privacy Rule or Security Rule. As noted above, the Final Rule specifically provides that subcontractors of business associates are themselves also business associates.	Business associates and their subcontractors should reconsider both their data privacy and security policies, procedures and safeguards and their data privacy and security risk assessments in light of the potential for direct liability for CMPs and criminal penalties.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications

Business Associate Agreement Provisions Required by Privacy Rule
 	
(45 CFR § 164.504(e))
	The current Privacy Rule requires a business associate agreement to do the following:
	
	▪ Establish the permitted and required uses and disclosures of PHI by the business associate. The contract may not authorize the business associate to use or further disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity, except for the following:
	  ▪ The contract may permit the business associate to use and disclose PHI for the proper management and administration of the business associate.
	  ▪ The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
	▪ Provide that the business associate will or will not do the following:
	  ▪ Will not use or further disclose PHI other than as permitted or required by the contract or as required by law
	  ▪ Will use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the agreement
	  ▪ Will report to the covered entity any use or disclosure of PHI not provided for by the agreement of which it
		The Final Rule amends the currently required business associate agreement provisions and adds new required provisions.
		
		Amendments to Current Provisions
		▪ The Final Rule amends the requirement that business associates report to the covered entity breaches of the business associate agreement to add a requirement to report to the covered entity breaches of unsecured PHI in accordance with the HITECH breach notification standards.
		▪ The Final Rule amends the Business Associate Agreement provision requiring the business associate to use appropriate safeguards by adding a requirement that the business associate comply with the Security Rule with respect to PHI maintained or transmitted in electronic media (EPHI).
		▪ The Final Rule clarifies the requirement that the business associate enter into a compliant downstream agreement with any subcontractor consistent with the revised definition of a business associate and the new definition of a "subcontractor."
		
		New Provision
		▪ To the extent business associate will carry out a covered entity's obligation under the Privacy Rule,
			Covered entities and business associates should undertake an inventory of all of their business associate arrangements (or subcontractor arrangements, in the case of business associates) to identify whether new business associate agreements are needed and whether existing business associate agreements need to be updated to comply with the Final Rule requirements for business associate agreements.
			
			Covered entities and business associates should develop new template business associate agreements consistent with the Final Rule requirements.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	becomes aware ▪ Will ensure that any agents and subcontractors to whom it provides PHI received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information ▪ Will make available PHI in accordance with the Privacy Rule standard establishing an individual's right to access PHI in medical records, billing records or other designated record sets ▪ Will make PHI available for amendment and incorporate any amendments to PHI in accordance with the Privacy Rule standard establishing an individual's right to amend PHI in a designated record set ▪ Will make available the information required to provide an accounting of disclosures in accordance with Privacy Rule's accounting standard ▪ Will make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the	the business associate agreement must require the Business Associate to comply with the Privacy Rule requirements that apply to covered entity's performance of the Privacy Rule obligation. ***Compliance Effective Date for Existing and New Business Associate Agreements*** Business associate agreements must comply with the new requirements in the Final Rule beginning September 23, 2013, except that a business associate agreement will be given a grace period with deemed compliance for one year (*i.e.*, until September 22, 2014) if both of the following apply: ▪ The business associate agreement is in place as of January 25, 2013 ▪ The business associate agreement is not reviewed or modified from March 26, 2013, until September 23, 2013 If a business associate agreement is renewed or modified from March 26, 2013, to September 22, 2014, the renewal or modification must include amendments to bring the business associate agreement into compliance with the Final Rule.	

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	covered entity available to the Secretary of HHS for purposes of determining the covered entity's compliance with the Privacy Rule ▪ Will, at termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible ▪ Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the agreement.		
Breach Notification Standards			
Definition of Breach5 **(45 CFR § 164.402)**	Under the Breach Rule, a covered entity must notify an individual and OCR of a breach of unsecured PHI. PHI is considered secure if it is rendered unusable, unreadable or indecipherable to unauthorized persons	The Final Rule amends the definition of breach contained in the Breach Rule with the goal of reducing the instances in which a covered entity may avoid notifying individuals of an acquisition, access, use or disclosure in violation of the Privacy Rule	Covered entities and business associates should examine their policies and procedures to ensure that they require: (i) the performance of a risk assessment in all cases of uses or disclosures of PHI in

[5] The first column of this row summarizes the Breach Rule published in the *Federal Register* by OCR on August 24, 2009.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	through the use of a technology or methodology specified by HHS in guidance issued under the HITECH Act. Likewise, a business associate must notify a covered entity of a breach of unsecured PHI. The Breach Rule defines a breach generally 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. The Breach Rule defines the phrase "compromises the security or privacy of the PHI" to mean poses a significant risk of financial, reputational or other harm to the individual.	to the affected individual and reporting the same to OCR. It eliminates the risk of harm standard included in the definition of "compromises the security or privacy of the PHI" and adds a regulatory presumption that any acquisition, access, use or disclosure of PHI in violation of the Privacy Rule is a breach. An acquisition, access, use or disclosure of PHI in violation of the Privacy Rule is not a breach if either of the following apply: ▪ One of the three exceptions discussed in section "Exceptions to Definition of Breach" applies. ▪ The covered entity or business associate demonstrates that there is a "low probability" that the PHI has been compromised based on the results of a risk assessment, which must take into account at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.	violation of the Privacy Rule (unless an exception applies); (ii) the consideration of the four required factors (and allow for the consideration of other factors that may be relevant in particular circumstances) when conducting a risk assessment of an impermissible use or disclosure; and (iii) that all risk assessments, and assessments of whether or not the impermissible use or disclosure fits within one of the three exceptions, are thoroughly documented in writing, particularly when there is a finding of a "low probability" that PHI was compromised. Covered entities and business associates must maintain written records of risk assessments for at least six years. Covered entities and business associates should revisit their vendor assessment tools and security risk assessments in light of the increased likelihood that an authorized use or disclosure of unsecured PHI would be a reportable breach. Covered entities and business associates should monitor the issuance of future OCR guidance on risk assessments.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
Exceptions to Definition of Breach6 **(45 CFR § 164.402)**	The Breach Notification Rule provides that acquisition, access, use or disclosure of PHI is not a breach under the following exceptions, the first three of which are included in the HITECH Act: ▪ Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule ▪ Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule ▪ A disclosure of PHI where a covered entity or business associate has a good-faith belief that an unauthorized person to whom the disclosure was made would not	The Final Rule eliminates the exception to the definition of breach for PHI that excludes individual's name, Social Security number and the other "direct identifiers" of the limited data set standard, as well as date of birth and zip code, and preserves the three HITECH Act exceptions included in the Breach Rule.	While the Final Rule deletes the breach definitional exception for an unauthorized disclosure that excludes the direct identifiers, date of birth and zip code, covered entities and business associates should take the exclusion of such identifiers into account when assessing (under the breach definition) whether an unauthorized disclosure presents more than a low probability that PHI was compromised.

[6] The first column of this row summarizes the Breach Notification Rule published in the *Federal Register* by OCR on August 24, 2009.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	reasonably have been able to retain such information ▪ A use or disclosure of PHI that excludes the direct identifiers of the limited data set standard, as well as date of birth and zip code, and did not compromise the security or privacy of the PHI		
Restrictions on Use of PHI for Marketing Communications			
Marketing Authorization **(45 CFR § 164.508)**	The Privacy Rule requires a covered entity to obtain an individual's Privacy Rule-compliant authorization prior to using or disclosing PHI about the individual for "marketing" (defined below) purposes *other than* one of the following: ▪ A communication made in a face-to-face conversation with the individual who is the subject of the PHI ▪ The provision of a promotional gift of nominal value to the individual If the covered entity making the marketing communication receives direct or indirect remuneration from a third party, the marketing authorization must state that the covered entity receives remuneration for the communication. The current Privacy Rule does not define "direct or indirect remuneration."	The Final Rule both implements the HITECH Act's amendments to the exceptions to the marketing authorization requirements and makes other changes that significantly increase the Privacy Rule's restrictions on the use of PHI for marketing. As in the current Privacy Rule, the Final Rule requires a covered entity to obtain an individual's authorization prior to using or disclosing PHI about the individual for "marketing" (defined below) purposes *other than* one of the following: ▪ A communication made in a face-to-face conversation with the individual who is the subject of the PHI ▪ The provision of a promotional gift of nominal value to the individual An authorization is not required for the face-to-face communications or promotional gifts, even if a third party pays the covered entity to make the communication or give the gift.	A covered entity should review its arrangements with third parties to identify any payments that the covered entity receives in exchange for making communications about the third party's products or services. Unless the communications concern drugs or biologics currently prescribed for the individual, the arrangements should be terminated or amended to comply with the new restrictions on receiving financial remuneration for marketing communications. In addition, pharmacies and other providers that conduct refill reminder or drug adherence programs in exchange for payments from drug or biologic manufacturers or other parties should review the financial terms to confirm that the payments are reasonably related to the covered entity's cost of making the refill reminders or other communications.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		If the covered entity making the marketing communication receives "financial remuneration" from a third party and a Privacy Rule-compliant authorization is required before making the communication, the authorization must state that the covered entity receives such remuneration for the communication. The Final Rule defines "financial remuneration" as direct or indirect payment from or on behalf of a third party whose product or service is being described. Financial remuneration does not include either (i) non-financial benefits such as in-kind benefits, or (ii) any payment for the treatment of an individual.	
Marketing Definition **(45 CFR § 164.501)**	The definition includes two categories of marketing: ***Category 1*** A communication about a product or service that encourages recipients of the communication to purchase or use the product or service, *other than* any one of the following (if otherwise permissible under the Privacy Rule): ▪ **Communications by a covered entity about its own products or services**. This is a communication made 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	The Final Rule's definition of marketing includes only one category. Marketing is any communication about a product or service that encourages recipients of the communication to purchase or use the product or service *other than* any one of the following (if otherwise permissible under the Privacy Rule): ▪ A communication with a refill reminder or information about a drug or biologic that is currently being prescribed for the individual if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of	

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	communication, including communications about the following: ▪ The entities participating in a health care provider network or health plan network ▪ Replacement of, or enhancements to, a health plan ▪ 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. For example, a mailing by a health plan to plan subscribers approaching Medicare-eligible age with materials describing the plan's Medicare supplemental plan and an application form is not marketing. ▪ **A communication made for treatment of the individual**. This may include, for example, a mailing by a pharmacy or other health care provider of prescription refill reminders to patients. ▪ **A communication made for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual.** For example, a hospital social worker's sharing of medical record information with nursing homes in the course of recommending that the patient be	making the communication. OCR states in the preamble commentary that it considers communications about generic equivalents to currently prescribed drugs or biologics to be within the scope of this exception. ▪ A communication for treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual if the covered entity does not receive financial remuneration in exchange for making the communication. Thus, a covered entity cannot receive payments for treatment communications except for cost-based payments for refill reminders and other communications about currently prescribed drugs or biologics. ▪ A communication describing 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 if the covered entity does not receive financial remuneration in exchange for making the communication. Without limitation, such unremunerated	

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	transferred from a hospital to a nursing home as part of hospital discharge planning is not marketing. ***Category 2*** An arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service. This category of marketing has no exceptions to the Privacy Rule's authorization requirement.	communications may describe the following: ▪ oThe entities participating in a health care provider network or health plan network ▪ oReplacement of, or enhancements to, a health plan ▪ oHealth-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits ▪ A communication for case management or care coordination for the individual, including 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 if the covered entity does not receive financial remuneration in exchange for making the communication. ***Payments for Other Purposes*** Under the Final Rule, a covered entity may continue to receive financial remuneration from a third party for purposes other than making marketing communications. For example, OCR notes in the Final Rule preamble that a covered entity may receive payments from a third party to implement a disease management program and communicate with individuals about the	

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		program without obtaining individual authorizations so long as the communications are about the program itself. This is because OCR draws a distinction between payments to help a covered entity set up a program, product or service and payments in exchange for marketing communications to individuals. However, in practice it may be difficult to distinguish between payments to support a program that involves communications with individuals and payments for the communications themselves.	
Sale of PHI			
Sale of PHI **(45 CFR § 164.502(a)(5)(ii))**	The current Privacy Rule does not contain an express, general prohibition on the sale of PHI. The concept is only indirectly encompassed within the definition of marketing that includes an arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.	As required by the HITECH Act, the Final Rule expressly requires a covered entity or business associate to obtain an individual's authorization for the "sale of PHI" about the individual. The Final Rule defines sale of PHI to mean a disclosure of PHI where the covered entity or business associate directly or indirectly receives remuneration, *in cash or in kind*, from (or on behalf of) the recipient of the PHI in exchange for the PHI unless the disclosure is for one of the eight purposes listed below: ▪ For public health purposes ▪ For research where the remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI ▪ For treatment and	Covered entities should update policies and procedures to reflect this new general prohibition on sale of PHI and the eight exceptions, and appropriately train on those policies and procedures. Covered entities should also identify and review all arrangements under which it discloses PHI to a third party in exchange for a fee for compliance with the sale of PHI prohibition. In particular, a covered entity should confirm that a business associate agreement does not involve payments for data in addition to fair market value compensation for business associate's services and confirm that research arrangements only involve reasonable cost-based fees to cover the cost to prepare and

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		payment purposes ▪ For the sale, transfer, merger or consolidation of all or part of the covered entity and related due diligence ▪ To or by a business associate (including a business associate that is a subcontractor) for business associate activities that the business associate undertakes on behalf of the covered entity (or business associate in the case of a subcontractor) and the only remuneration provided is for the performance of the business associate's activities ▪ To the individual under the individual rights to access and an accounting ▪ As required by law ▪ For any other purpose permitted by HIPAA, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law In the Final Rule preamble, OCR notes that a sale of PHI includes transactions where the disclosing covered entity or business associate does not transfer title to the PHI. Therefore, license and other arrangements granting access and use rights will also be considered a sale.	transmit PHI (or meet another exception). Review of research arrangements should include consideration of the extent to which the value of PHI license, access and use rights might exceed the reasonable cost to prepare and transmit the PHI.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
Restrictions on Fundraising Communications			
PHI That May be Used for Fundraising Purposes **(45 CFR § 164.514(f))**	The current Privacy Rule permits a covered entity (such as a tax-exempt health care provider) to use or disclose to a business associate, or to an institutionally related foundation, certain limited categories of PHI for fundraising purposes, including demographic information relating to an individual and dates of health care provided to an individual. Prior to the issuance of the Final Rule, OCR stated in industry guidance that, although "demographic information" is not defined in the Privacy Rule, demographic information includes the individual's name, address and other contact information, age, gender, and insurance status.	Like the current Privacy Rule, the Final Rule permits a covered entity to use or disclose to a business associate, or to an institutionally related foundation, certain limited categories of PHI for fundraising purposes. The Final Rule clarifies and expands the types of information that may be used and disclosed for fundraising purposes and makes other changes with respect to a patient's rights to avoid unwanted fundraising solicitations. The Final Rule allows the use and disclosure of the following types of PHI for fundraising: ▪ Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth (as permitted under the current Privacy Rule) ▪ Dates of health care provided to an individual (as permitted under the current Privacy Rule) ▪ Department of service information ▪ Treating physician information ▪ Outcome information ▪ Health insurance status ***No Conditioning of Treatment*** The Final Rule prohibits the conditioning of treatment or payment on an individual's choice with respect to the	Covered entities should consider revising their fundraising policies and procedures to permit use of the expanded types of PHI for fundraising authorized under the Final Rule, and appropriately train on the revised policies and procedures.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		receipt of fundraising communications.	
Right to Opt Out of Fundraising Communications **(45 CFR § 164.514(f))**	A covered entity must include in any fundraising materials a description of how the individual may opt out of receiving any further fundraising communications. If an individual opts out, the covered entity must make reasonable efforts to ensure that the individual does not receive future fundraising communications.	Like the current Privacy Rule, the Final Rule requires a covered entity to provide an individual with an opportunity to opt out of fundraising communications. To clarify that the opt-out requirement applies to fundraising solicitations made over the phone, the Final Rule provides that the opt-out requirement applies to each fundraising communication "made" and not only to materials "sent" to an individual. The Final Rule permits a covered entity to choose the opt-out methodology, provided that the method does not impose an undue burden or more than a nominal cost on individuals who want to opt out. ▪ In the Final Rule preamble, OCR suggests that covered entities consider the use of a toll-free phone number, an e-mail address, and/or similar opt-out mechanisms that provide individuals with simple, quick and inexpensive ways to opt out of receiving further fundraising communications. OCR also states that requiring individuals to opt out by mailing a pre-printed, pre-paid postcard would not constitute an undue burden under the Final Rule, but that requiring individuals to write a letter	Covered entities should review their method(s) for enabling individuals to opt out from fundraising communications to ensure that the method(s) are clear and conspicuous and do not impose an undue burden, nor more than a nominal cost, on an individual. In addition, covered entities should ensure that both written and oral (*e.g.*, telephone solicitations) fundraising communications comply with the opt-out requirements. Since the Final Rule requires strict compliance with individuals' opt outs, a covered entity (including an affiliated covered entity of multiple covered entities) that conducts fundraising activities through multiple departments should consider implementing an enterprise-wide system for tracking opt outs. Covered entities should review and revise their HIPAA policies and procedures to address the revised opt-out requirements and strict compliance standard, and appropriately train on the revised policies and procedures.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		to opt out would constitute an undue burden. Unlike the current Privacy Rule, which requires a covered entity to make reasonable efforts not to send fundraising communications to individuals who have opted out, the Final Rule requires strict compliance with an opt-out request. The Final Rule provides that a covered entity may provide a method for individuals to opt back into receiving fundraising communications.	
Notice of Privacy Practices Requirements for Fundraising **(45 CFR § 164.520)**	In order to use demographic information and dates of service for fundraising purposes, the covered entity must include a statement to that effect in its notice of privacy practices.	The Final Rule maintains the requirement that a covered entity include a statement regarding its use of PHI for fundraising purposes in its notice of privacy practices, and adds the requirement to describe an individual's right to opt out of receiving fundraising communications from the covered entity.	A covered entity that uses PHI for fundraising purposes should ensure that its notice of privacy practices includes a statement regarding such use and describes how the individual may opt out of receiving fundraising communications.
Use and Disclosure of PHI for Research and Other Future Use			
Research and Other Future Use of PHI—Compound Authorizations **(45 CFR § 164.508(b))**	***Compound Form Ban*** The current Privacy Rule prohibits an authorization from being combined with any other document, unless an exception applies (the so-called Compound Form Ban). One exception permits an authorization for the use and disclosure of PHI in connection with a research study to be combined with the informed consent document *for the same study*. ***Conditional Authorization Ban***	***Compound Form Ban*** The Final Rule does not change this general rule and the research-related exception. ***Conditional Authorization Ban*** The Final Rule does not change this general rule and the research-related exception. ***Single Form Combining Conditional and Unconditional Authorizations*** The Final Rule now permits	The changes to the Final Rule with respect to compound forms harmonizes the Privacy Rule's research authorization requirements and standards with existing practice under the Common Rule. As such, the Final Rule will likely be welcomed by the research community. To take advantage of the greater flexibility allowed by the Final Rule, covered entities will want to update the design and operation of

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	The current Privacy Rule also prohibits a covered entity from conditioning treatment or payment on an individual's signing of an authorization, unless an exception applies (Conditioning Ban). One exception is that a covered entity may condition an individual's receipt of the study intervention (*e.g.*, research-related treatment involving an investigational device or drug) on the individual's signing of an authorization for the use and disclosure of that individual's PHI *in connection with the same study*. ***Ban on Combining Conditional and Unconditional Authorizations*** The current Privacy Rule prohibits a covered entity from combining conditional and unconditional authorizations into a single form. Thus, for example, a covered entity could not use the same authorization form *both* to (i) authorize the use of PHI in conducting a primary study (*e.g.*, a study of the safety and efficacy of a new chemotherapy regimen for pancreatic cancer), which authorization could condition treatment on participation in the primary study, and (2) authorize the voluntary participation in a secondary study (*e.g.*, the creation of a repository containing excess tissue and associated PHI collected in the course of the primary study), which authorization could not condition treatment or the ability to participate in	a covered entity to combine conditional and unconditional authorizations for research into a single authorization form, provided that the compound authorization clearly differentiates between the conditional and unconditional elements and clearly allows the individual to opt into the unconditioned elements. (An opt-in approach requires researchers to explicitly ask subjects to affirmatively elect to participate in the unconditional component). The unconditional component can be for "any type of research activities." An authorization for research involving the use and disclosure of psychotherapy notes, however, may only be combined with another authorization for the use and disclosure of psychotherapy notes. The Final Rule allows covered entities and Institutional Review Boards (IRBs), the committees that oversee human research protections, flexibility in determining how best to distinguish clearly between the conditional and unconditional research components described in a single authorization. However, this discretion cannot be exercised in favor of permitting covered entities and IRBs to utilize an opt out approach to the unconditional element(s). OCR believes that an opt out approach does not provide individuals with sufficient ability to understand that they may decline the	their research compliance programs to integrate these new requirements, through the following: ▪ Developing new policies and procedures with respect to compound forms and unspecified future use ▪ Developing new template informed-consent authorization forms that integrate both conditional and unconditional elements and provide for future unspecified use ▪ Developing and providing training for IRB members on how to review compound informed-consent authorization forms to ensure that subjects are clearly informed about those aspects of the study in which they can decline to participate while still being enrolled

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	the primary study, on participation in the secondary study. Rather, a research participant would need to sign two, separate authorizations if the individual wished to participate in both research activities.	unconditional elements. Covered entities are permitted, but not required, to use the compound authorization. Ongoing studies may continue to rely on separate authorizations. OCR explicitly states in the Final Rule preamble that it intends for these amendments to result in the use of compound authorizations combining conditional and unconditional elements for, but not limited to, use of PHI to create data banks and bio-repositories. A research subject may revoke only one part of a compound authorization, provided that it is clear that the individual wishes to only revoke a portion of the authorization. If it is not clear whether the revocation is for all or part of a compound authorization, covered entities must obtain clarification from the individual as to whether the individual wishes to revoke all or just part of an authorization. If this clarification is not obtained, then the entire authorization must be treated as revoked.	
Research and Other Secondary Use of PHI—Specificity of Description of Use for Future Research Purposes **(45 CFR § 164.508(b) and (c))**	The current Privacy Rule requires an authorization to be specific as to the purpose of any authorized uses or disclosures. OCR previously interpreted the purpose requirement as it relates to research studies to require an authorization to reference a particular study when describing the research purposes for which PHI	The Final Rule does not change the requirement that a valid authorization must include a description of each "purpose" of a requested use and/or disclosure of PHI. OCR states in the Final Rule preamble, however, that it will no longer interpret the "purpose" requirement to mean that an authorization must identify a specific study	The changes to the Final Rule with respect to unspecified future use harmonize the HIPAA research authorization requirements and standards with existing practice under the Common Rule. As such, the Final Rule will likely be welcomed by the research

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	would be used and disclosed. Therefore, in connection with the conduct of any future research or research-related activities using PHI from a primary study, researchers may have been able to identify with specificity the intent to create a data repository as a secondary study when obtaining a an authorization for a primary study. However, with regard to future uses of data maintained in the repository, researchers have had to rely on other Privacy Rule use and disclosure pathways to avoid having to re-contact individuals to obtain new authorizations in the future when conducting research using PHI in the database (*e.g.*, Institutional Review Board (IRB) waiver of authorization, de-identification or creation of a limited data set).	for which the PHI will be used. Rather, the purpose may involve a general description of the purposes of the potential future research use(s). OCR further states that the intended purpose will be considered adequately described if "it would be reasonable for the individual to expect that his or her [PHI] could be used or disclosed for future research purpose." OCR explains that this adequate description might be achieved using specific statements with respect to sensitive research if such research is anticipated, but the Final Rule does not require any such specific statements. Covered entities and IRBs thus retain considerable discretion as to whether a description of future use is adequate. The preamble also clarifies that the description of the PHI to be used in future use may extend to PHI not yet collected at the time the authorization is signed. Finally, the preamble reminds and cautions covered entities that OCR's modification of its interpretation of the purpose requirement does not change the overarching required elements of a valid authorization even if, with respect to future use, they "are to be described in a more general matter." After the effective date of the Final Rule, covered entities may elect to use study-	community. To take advantage of the greater flexibility allowed by the Final Rule, covered entities will want to update the design and operation of their research compliance programs to integrate these new requirements, through the following: ▪ Developing and providing training for IRB members on future use and on how to review informed-consent authorization forms to ensure that all elements of a valid authorization, as pertaining to the future use component, are adequately addressed ▪ Developing case studies and other guidelines to assist IRBs and institutions with structuring flexible and broad-reaching future use programs while still preserving meaningful and informed consent by subjects ▪ Establishing tracking and flagging mechanisms to distinguish between bio-specimens collected prior to the effective date of the Final Rule (for which there is no ability to use an authorization for future, unspecified use) and biospecimens collected after the effective date (for which there is authorization for future use) ▪ Developing freestanding

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		specific authorizations or new authorizations that contemplate future use. In addition, covered entities and researchers may continue to rely on any IRB-approved consents obtained prior to the Final Rule effective date that "reasonably informed" individuals of potential future use, provided that "the informed consent was combined with a HIPAA authorization."	informed-consent authorization forms addressing future use that can be used in connection with routine intake packets to expand the versatility and diversity of biobanking initiatives
Research and Other Secondary Use of PHI—Specificity of Description of Use for Future Research Purposes **(45 CFR § 164.508(b) and (c))**	The current Privacy Rule does not address the sale of PHI in connection with research.	As required by the HITECH Act, the Final Rule prohibits the sale of PHI unless an exception applies. The HITECH Act and the Final Rule include an exception for the sale of PHI in connection with research under limited circumstances. Specifically, a covered entity need not have prior valid authorization if the remuneration is in connection with a research study and such compensation is limited to the "reasonable cost" of preparing and transmitting the PHI, but is not for the PHI itself. According to the preamble, these reasonable costs can be direct or indirect expenses incurred by the covered entity. Also noteworthy is that, unlike the exceptions in the Final Rule regarding the use of PHI for marketing activities, the reasonable cost standard applicable to remuneration for the sale of PHI in connection with research counts *both financial remuneration and in-kind*	With respect to the clarified sale of PHI provisions relating to research, covered entities and life science companies should establish prospective, cost-based price lists that encompass only the covered entity's costs in accessing, collecting, processing, analyzing and transmitting PHI but that do not assign value to the PHI itself and do not result in a profit to the covered entity. They should watch for additional Department guidance on the "appropriate cost-based limitations on remuneration." Research agreements and associated budgets should take care to describe the services involving PHI for which compensation is paid and should clearly establish that the compensation is for these services and is not consideration for the PHI itself. The remuneration concept in the Final Rule relating to

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		remuneration. The preamble states that OCR intends to issue additional guidance on the "appropriate cost-based limitations on remuneration." OCR will grandfather ongoing research studies that were initiated "based on a prior permission under the Privacy Rule." Section 164.508(a)(4) explicitly states that the transition provisions set forth as 164.532 apply to permissions existing prior to the applicable date of the Final Rule. Further, Section 164.532(f) states that a covered entity may continue to use and/or disclose a limited data set in accordance with a data use agreement entered into prior to the effective date of the Final Rule that provides for a sale of PHI until such data use agreement is renewed or until one year from the compliance date of this Final Rule, whichever is earlier. See also the general discussion regarding the sale of PHI set forth above.	the research exception to the sale of PHI prohibition creates special challenges for collaborative studies involving equipment leave-behinds and the contribution of PHI by a covered entity to a data bank in return for rights to access and use the data bank. OCR notes in the Final Rule preamble that some commenters expressed concern that prohibiting indirect remuneration and/or non-financial benefits, absent authorization, may chill participation in collaborative data initiatives. However, OCR does not indicate whether the "membership" benefits in such a collaboration would constitute remuneration. Limiting reasonable remuneration to costs suggests that if the fees received generate a "profit," then the amount of the remuneration would trigger the authorization requirement even if the amount charged does not exceed fair market value. Covered entities should monitor the issuance of additional guidance on the "appropriate cost-based limitations on remuneration," particularly with regard to whether and how PHI license, access and use rights must be factored into the determination of cost.
Enforcement			

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
Amount of CMP **(45 CFR § 160.404)**	The Interim Enforcement Rule amended the Enforcement Rule to include the imposition of four tiered ranges for civil money penalty amounts based upon the increasing levels of culpability associated with violations of HIPAA administrative simplification provisions occurring after February 18, 2009, and make certain other changes consistent with the HITECH Act. The tiered ranges for civil money penalty amounts are as follows: ▪ $100 to $50,000 for each violation of a HIPAA administrative simplification provision where the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that it violated the provision ▪ $1,000 to $50,000 for each violation of a HIPAA administrative simplification provision that is due to reasonable cause and not to willful neglect ▪ $10,000 to $50,000 for each violation of a HIPAA administrative simplification provision that 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 ▪ $50,000 to $1,500,000 for each violation of a HIPAA administrative simplification provision that is due to willful neglect and was not corrected during the 30-day period beginning on	The Final Rule adopted in full the changes made under the Interim Enforcement Rule. For additional information regarding the Interim Enforcement Rule, see McDermott's *On the Subject* "HHS Issues Interim Final Rule Conforming HIPAA Civil Money Penalties to HITECH Act Requirements."	Covered entities and business associates should update policies and procedures, appropriately train their workforce on such policies and procedures, and take any other necessary steps to ensure that they are meeting their obligations under the administrative simplification provisions. Covered entities and business associates should position themselves to react swiftly upon learning of a HIPAA violation in order to correct the violation quickly and mitigate any resulting harm. These factors can directly impact which tier a violation falls into and the potential penalty amount. Covered entities and business associates should conduct reasonable due diligence on the privacy and security practices of business associates and their subcontractors, particularly those that receive significant amounts of PHI or categories of PHI that are particularly sensitive (*e.g.*, Social Security numbers or mental health information).

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
Applicability of Enforcement Rule to Business Associates **(45 CFR §§ 160.300)**	Prior to the HITECH Act, business associates were not directly subject to the HIPAA civil and criminal penalty scheme. Instead, covered entities were required to impose certain privacy and security obligations on business associates contractually through written contracts containing certain business associate agreement requirements. Accordingly, the Enforcement Rule was not directly applicable to business associates. As required by the HITECH Act, the Interim Enforcement Rule amended the Enforcement Rule to make it directly applicable to business associates. To account for the direct application of the regulations to business associates, the Interim Enforcement Rule revised a number of sections of the Enforcement Rule by adding the term "business associate."[7]	The Final Rule adopted in full the changes made under the Interim Enforcement Rule.	Business associates should reconsider their data privacy and security policies, procedures and safeguards and their data privacy and security risk assessments in light of the potential risk of civil and criminal liability.
Vicarious Liability for Violations of an Agent **(45 CFR § 160.402)**	Under the current Privacy Rule, covered entities are subject to a civil money penalty for a violation of the Privacy Rule or Security Rule. The Privacy Rule provides that violations of another entity such as a business associate are attributed to a covered entity in accordance with federal common law of	The Final Rule revises the standard for determining whether a covered entity is vicariously liable for the HIPAA violations committed by another person such as a business associate: ▪ Covered entity liability for acts or omissions of its agents now extends to the acts or omissions of its business associates, in	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 achieved by conducting a vendor

[7] For additional information regarding the Interim Enforcement Rule, see McDermott's *On the Subject* "HHS Issues Interim Final Rule Conforming HIPAA Civil Money Penalties to HITECH Act Requirements," available at www.mwe.com/publications/uniEntity.aspx?xpST=PublicationDetail&pub=5322&PublicationTypes=d9093adb-e95d-4f19-819a-f0bb5170ab6d.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
	agency for violations based on the act or omission of any agent of the covered entity, including a workforce member, acting within the scope of agency, *except that* the covered entity is not liable if the following apply: ▪ The agent is a business associate. ▪ The covered entity has entered into a compliant business associate agreement with the agent. The covered entity did not know of a pattern or practice of the business associate in violation of the contract and did not fail to act as required by the Privacy Rule or Security Rule with respect to such violations.	accordance with the federal common law of agency, regardless of whether the relevant business associate agreement requirements have been met. ▪ Business associates are now likewise liable for acts or omissions of any agent of the business associate, including workforce members and subcontractors, in accordance with the federal common law of agency. In the Final Rule preamble, OCR states that the key factor in determining vicarious liability is whether the principal (*i.e.*, the covered entity with respect to a business associate or the business associate with respect to subcontractor) has authority to control the agent's conduct in the course of performing a service on behalf of principal. OCR identifies the following indicia of an agency relationship: ▪ The principal has authority to give interim instructions or directions ▪ The principal can direct the performance of a service after a business associate agreement is signed ▪ The covered entity delegates a HIPAA obligation to the business associate In contrast, the Final Rule	privacy and security assessment in advance and by carefully structuring business associate agreements and downstream subcontractor agreements to provide an appropriate level of oversight.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		preamble states that an independent contractor relationship may exist if the only avenue of control is for the principal to amend the terms of the business associate agreement or sue for breach. The principal is not liable for the violations of a business associate that is an independent contractor unless the principal knew of a pattern or practice of breach of the business associate agreement.	
OCR Investigations and Compliance Reviews **(45 CFR §§ 160.306, 160.308, 160.312)**	The Enforcement Rule provides that OCR *may, but is not required to*, conduct complaint investigations or compliance reviews to determine whether a covered entity is complying with an administrative simplification provision. The Enforcement Rule *requires* OCR to attempt to resolve by informal means investigations or compliance reviews that indicate non-compliance.	The Final Rule *requires* OCR to conduct an investigation or compliance review when a preliminary investigation of the facts indicate a possible violation due to willful neglect (*i.e.*, the third and fourth culpability levels under the civil money penalty provisions), and retains OCR's discretion to conduct such reviews in circumstances where a preliminary investigation does not indicate a possible violation due to willful neglect. While the Enforcement Rule did not previously require OCR to investigate all complaints, OCR states in the Final Rule preamble that, as a practical matter, it currently proceeds with investigations in all cases where an initial review indicates a possible HIPAA violation. The Final Rule *permits*, but does not require, OCR to attempt to resolve by informal means investigations or compliance reviews that indicate non-compliance. The purpose of this change is to grant OCR	Covered entities and business associates should reconsider their data privacy and security risk assessments in light of OCR's enhanced enforcement authority and a recent increase in OCR enforcement actions resulting in settlement payments.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		the discretion to proceed directly to the imposition of a civil money penalty without exhausting informal resolution efforts (particularly in cases involving willful neglect).	
Factors Considered in Determining the Amount of a Civil Money Penalty (CMP) **(45 CFR § 160.408)**	The Enforcement Rule provides OCR with the discretion to decide whether and how to consider (as either mitigating or aggravating) the following factors in determining the amount of a civil money penalty: ▪ The nature of the violation ▪ The circumstances of the violation ▪ The degree of culpability of the covered entity ▪ The history of prior offenses ▪ The financial condition of the covered entity ▪ Such other matters as justice may require	The Final Rule amends the factors that OCR must consider under the Enforcement Rule to determine the amount of a civil money penalty consistent with the HITECH Act and as otherwise deemed appropriate. Under the Final Rule, the OCR must consider the following factors in determining the amount of a civil money penalty: ▪ The nature and extent of the violation, consideration of which may include but is not limited to the number of individuals affected and the time period during which the violation occurred ▪ The nature and extent of the harm resulting from the violation, including, without limitation, whether the violation caused physical harm, resulted in financial harm, resulted in harm to an individual's reputation, and hindered an individual's ability to obtain health care ▪ The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, including, without limitation, whether the current violation is the	Covered entities and business associates should update policies and procedures, appropriately train their workforce on such policies and procedures, and take any other necessary and/or reasonable steps to ensure that they are meeting their obligations under the administrative simplification provisions. Covered entities and business associates should ensure that they are in a position to react swiftly upon learning of a HIPAA violation in order to correct the violation quickly and mitigate any resulting harm. These factors can directly impact which tier a violation falls into and the potential CMP amount.

Topic	Current HIPAA Regulations	Final Rule	Operational and Other Implications
		same or similar to previous indications of noncompliance, whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance, how the covered entity or business associate has responded to technical assistance from OCR provided in the context of a compliance effort, and how the covered entity or business associate has responded to prior complaints ▪ The financial condition of the covered entity or business associate, consideration of which may include but is not limited to, whether the covered entity or business associate had financial difficulties that affected its ability to comply, whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care, and the size of the covered entity or business associate ▪ Such other matters as justice may require	

For more information regarding the final modifications to the HIPAA Privacy, Security, Breach Notification and Enforcement Rules to implement the HITECH Act and how they may affect your business, please contact your regular McDermott Will & Emery lawyer or one of the authors:

Bernadette M. Broccolo: + 1 312 984 6911 bbroccolo@mwe.com

Daniel F. Gottlieb: +1 312 984 6471 dgottlieb@mwe.com

Jennifer S. Geetter: +1 202 756 8205 jgeetter@mwe.com

Ryan S. Higgins: +1 312 984 2052 rshiggins@mwe.com

Amy Hooper Kearbey: +1 202 756 8069 akearbey@mwe.com

Edward G. Zacharias: +1 617 535 4018 ezacharias@mwe.com

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