

# Regulatory Update: HITECH's HHS and FTC Security Breach Notification Requirements

August 27, 2009

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), part of the American Recovery and Reinvestment Act of 2009, includes significant investment in health information technology (IT) to facilitate the adoption of a nationwide health information network. Recognizing that the expansion of health IT creates the need for additional safeguards to protect personal information, among other measures, the HITECH Act requires covered entities, business associates, vendors of personal health records (PHR) and related entities to notify individuals when their unsecured protected health information (PHI) and PHR identifiable health information is subject to a breach of security.

The HITECH Act provides a framework for these security breach notification requirements and directs both the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) to promulgate further regulations. HHS and FTC have recently issued rules relating to these security breach notification requirements. The two agencies consulted with one another to harmonize their respective security breach notification rules. Compliance with these regulations will require the expenditure of significant time and expense, and, therefore, health care and related industries should begin immediately familiarizing themselves with the rulemakings and updating their processes and procedures to comply accordingly.

For additional information regarding the security breach notification requirements set forth in the HITECH Act, see McDermott's *White Papers* "Economic Stimulus Package: Policy Implications of the Financial Incentives to Promote Health IT and New Privacy," available at <http://www.mwe.com/info/news/wp0209e.htm>, and "Regulatory Update: HITECH's Security Breach Notification Requirements," available at <http://www.mwe.com/info/news/wp0409e.pdf>.

## HHS Breach Notification Interim Final Rule

Following its April 2009 Guidance on the HITECH Act's requirements, HHS recently issued an "Interim Final Rule" on security breach notification requirements (available at <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>). HHS waived the notice and comment requirements of the Administrative Procedure Act and issued the Interim Final Rule without first issuing a proposed rulemaking on the subject. HHS explained that it had "good cause" to issue an Interim Final Rule in this instance because the HITECH Act "explicitly required" HHS to issue the regulations as interim final regulations within 180 days of the Act's promulgation. Based on the directive in the Act and the limited time frame involved, HHS concluded that notice and comment rulemaking was impracticable and contrary to public policy. However, HHS is accepting public comments on the Interim Final Rule within a 60-day period after publication of the Interim Final Rule. The Interim Final Rule will be codified as a new subpart D to 45 CFR Part 164.

The Interim Final Rule focuses on three principal topics:

- Reviewing the applicability of the Rule, its interplay with the FTC Health Breach Notification Rule, and its relationship with the Security and Privacy Rules promulgated pursuant to HIPAA (45 CFR 164, Parts C and E, respectively)
- Updating its prior guidance on the technologies and methodologies that render health information "unusable, unreadable or indecipherable" to unauthorized persons
- Elaborating on specific statutory and regulatory provisions

Throughout the Rule, HHS reiterates that, while compliance with the Privacy and Security Rules of HIPAA remains mandatory, covered entities and business associates, at their discretion, may opt to adopt technologies and methodologies to render health information "unusable, unreadable or indecipherable." Although adoption of these stricter protections is optional, covered entities and business associates that have unsecured PHI—*i.e.*, PHI that has not been acceptably rendered unusable, unreadable or indecipherable—will need to comply with notice provisions in the event of a breach. Neither the April Guidance nor the Interim Final Rule modifies a covered entity's responsibilities under the Privacy and Security Rule. The Security Rule's requirements regarding encryption remain. However, as the Interim Final Rule points out, the Security Rule's encryption requirement is "addressable" (as opposed to required), and, therefore, covered entities have a certain amount of discretion in the encryption technology adopted. Under the Interim Final Rule, such discretion remains; however, if the covered entity or business associate wishes to avoid the breach notification provisions, it will have to adopt the security technologies and methodologies set forth in the April Guidance to ensure that individually identifiable information is properly encrypted.

## RESPONSE TO THE APRIL GUIDANCE

In response to the April Guidance, HHS received a number of comments and suggestions regarding the acceptable technologies and methodologies for destruction. In response to such comments, HHS took the following action:

- Provided clarification regarding the forms of information addressed in the National Institute of Standards and Technology (NIST) publications referenced in the April Guidance
- Clarified the meaning of “data in motion,” “data in use” and “data at rest”
- Declined to include access controls as a recognized method for rendering PHI secured, because, although access controls can be effective in securing PHI and may render PHI inaccessible to unauthorized persons, in the event that a breach occurs, access controls will not render the PHI unusable, unreadable or indecipherable as required by the Act
- Declined to include redaction of paper records as an alternative to destruction of such records, because HHS concluded that redaction was not a “proven” methodology for rendering information unusable, unreadable or indecipherable
- Confirmed that covered entities and business associates may continue to use redaction as a means of creating limited data sets and de-identified data sets and that, in certain cases, a breach of unsecured PHI in the form of a limited data set may not trigger the notification requirements because the data set does not compromise the security or privacy of the individual to whom the information pertains
- Clarified that entities should retain encryption keys on a separate device from the one housing the encrypted data

Section 13402(h) of the Act defines unsecured PHI as PHI that has not been secured “through the use of a technology or methodology specified by the Secretary in guidance.” The Secretary issued this guidance on April 17, 2009, specifying the encryption and destruction technologies and methodologies that would render PHI secured, and, therefore, not subject to the breach notification requirements.

## ENCRYPTION

PHI is rendered unusable, unreadable or indecipherable if it is encrypted or destroyed in compliance with the standards announced by the Secretary. “Encrypted” PHI refers to PHI that through “the use of an algorithmic process” has been transformed “into a form in which there is a low probability of assigning meaning without use of a confidential process or key,” and such process or key has not been breached. NIST has tested and verified encryption processes that meet this standard. PHI has been sufficiently destroyed if, in paper form, it has been shredded or otherwise destroyed such that the PHI “cannot be read or otherwise be reconstructed” and, if in electronic form, it has been “cleared, purged or destroyed” consistent with standards set forth by NIST. For additional information regarding encryption, see McDermott’s *White Paper* “Regulatory Update: HITECH’s Security Breach Notification Requirements,” available at <http://www.mwe.com/info/news/wp0409e.pdf>.

## BREACH

The HITECH Act defines “breach” as the “unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” The Interim Final Rule clarifies the statutory definition of “breach” as follows:

- Breach is the “acquisition, access, use or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information.”
- Breach is limited to protected health information; therefore inadvertent or unauthorized use or disclosure of de-identified information or of certain types of individually identifiable health information excluded from the definition of protected health information would not constitute a breach for this subpart.

- The meaning of the statutory reference to “unauthorized” is any use or disclosure not permitted by the Privacy Rule.
- The statutory references to “acquisition” and “access” are synonymous with the regulatory definitions of “use” and “disclosure” set forth in the Privacy Rule; the regulatory definition retains the terms “acquisition” and “access” solely to achieve linguistic consistency with the statutory language.
- Every violation of the Privacy Rule or Security Rule will not constitute a “breach” for purposes of the notification requirements; such violations, however, may make breaches more likely.
- Use or disclosure of PHI that is more than the minimum necessary amount may, without more, constitute a “breach” for purposes of the notification requirements.

The Interim Final Rule confirms that the first step in determining whether a breach has occurred is to determine whether there has been a use or disclosure of PHI that is not permitted by the Privacy Rule. If such a use or disclosure has occurred, the next step is to determine whether such use or disclosure “compromises the security or privacy” of the protected health information. The Act specifically limits the definition of “breach” to those situations in which such a compromise of security or security has occurred. In order to avoid covered entities and business associates notifying affected individuals when there has been any compromise, even a *de minimus* one, HHS interprets the statutory language to implicitly include a “harm threshold.” Therefore, HHS reads the phrase “compromises the security or privacy of the protected health information” to mean “poses a significant risk of financial, reputational, or other harm to the individual.” This harm threshold is intended to align the HHS security breach notification requirements with the breach notification laws of many states and existing obligations on certain federal agencies.

#### RISK ASSESSMENT

In order to determine whether there has been a significant risk of harm, covered entities and business associates must undertake a risk assessment. The Interim Final Rule sets forth a number of the factors that may be relevant in conducting the assessment:

- Who impermissibly used and/or received the PHI? Is the user/recipient subject to HIPAA or similar privacy protections?
- Did the covered entity or business associate have the opportunity to mitigate the impermissible use or disclosure? If so, were these mitigation steps effective at eliminating or reducing the risk of harm to the individual?
- Was the PHI returned prior to being accessed improperly?
- What was the type and amount of the PHI involved in the improper use or disclosure? Was it the type of information that alone or in combination with other disclosed data points is likely to pose a significant risk of harm?

The covered entity must document this risk assessment so that it can demonstrate, if necessary, that no notification of a breach was required following impermissible use or disclosure of PHI.

#### LIMITED DATA SETS

HHS had requested comments on whether a limited data set, which is a PHI data set created by removing 16 specific identifiers, should be deemed unusable, unreadable or indecipherable. HHS received a number of comments encouraging HHS to conclude that a limited data set was *per se* secured PHI. After reviewing the comments, HHS declined to agree but noted that an impermissible use or disclosure of a limited data set might not constitute a breach if the entity determines that such disclosure does not post a significant harm to the individual. In addition, HHS announced a “narrow, explicit exception” that an impermissible use or disclosure of a limited data set that also excludes dates of birth and zip codes is deemed not to compromise the security or privacy of the PHI. Finally, in the event that the impermissible use or disclosure of PHI in the form of a limited data set is determined to constitute a breach but it is not possible to identify the individuals sufficiently to provide specific notice, the covered entity or business associate must provide “substitute notice” as set forth in the Act.

## EXCEPTIONS

The Act also provides three exceptions to the definition of breach: unintentional use by employees or agents of the disclosing covered entity/business associate, inadvertent disclosures to similarly situated individuals within the same facility, and where the unauthorized recipient of the unsecured PHI cannot reasonably be expected to be able to retain it. The Interim Final Rule elaborates upon these three exceptions:

- With respect to the first exception, the unintentional use must be by a workforce member (which includes employees, volunteers, *etc.*) or individual acting “under the authority of the covered entity or business associate” and who used the PHI in good faith and within the scope of his or her employment or professional relationship. Moreover, the unintentional use cannot result in further use or disclosure.
- With respect to the second exception, the Interim Final Rule broadens the exception to include the same covered entity or business associate or organized health care arrangement (rather than only the same facility). The Interim Final Rule also clarifies that two people are “similarly situated” if they are both authorized to access PHI, even if they are not authorized to access the same types of PHI. Moreover, the PHI cannot be further used or disclosed in a manner that itself violates the Privacy Rule.
- With respect to the third exception, the Interim Final Rule clarifies that the exception applies to situations where a covered entity or business associate has a “good faith belief” that the recipient could not reasonably have been able to retain the PHI.

In all three exceptions, the covered entity or business associate bears the burden of proof to meet the requirements of the exception. A covered entity or business associate may take a “reasonable amount of time” to determine whether the impermissible use or disclosure constitutes a breach. The breach “occurs,” however, at the time of the use or disclosure, not at the moment that the covered entity or business associate completes this analysis. The Interim Final Rule also discusses how notice is to be shared with the relevant covered entity or entities by a business associate when the business associate experiences a breach.

## NOTICE OBLIGATIONS

Once a covered entity or business associate has determined that an impermissible use or disclosure has occurred, such use or disclosure poses a significant risk of harm to the individuals, and no exceptions apply, the covered entity or business associate must assess its notice obligations. The Interim Final Rule contains a number of important clarifications with respect to these notice obligations:

- As a general rule, a covered entity must notify every individual whose unsecured PHI has been breached following the discovery of the breach.
- A breach is “discovered” by a covered entity as of the “first day that the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity.”
- The breach is “known” if it is known, or could have been known using reasonable diligence, by “any person, other than the person committing the breach, who is a workforce member or agent of the covered entity.”
- Reasonable diligence is defined to be the “business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.”
- Covered entities and business associates are encouraged to implement reasonable systems for detecting breaches in order to comply with the constructive notice provisions.
- Notice must be sent no later than 60 days of discovery of a breach, but if the covered entity could reasonably conclude its investigation and send notice prior to 60 days, it may not be appropriate to allow the entire time to elapse.

- The notification must include, to the extent possible, a description of what happened, including the date of the breach; a description of the unsecured PHI; recommended steps for individuals to take to mitigate potential harm; a description of what the covered entity is doing in response; and contact information.
- Under certain circumstances, it may not be possible to provide individual notice to each affected person; in such cases, the Interim Final Rule sets forth how to issue substitute notice through the internet and appropriate media outlets.
- Notification can be delayed at the request of law enforcement if it would impede a criminal investigation or undermine national security.
- Finally, in the event that the breach involves PHI from 500 or more individuals, the covered entity must also notify the Secretary concurrently with notifying the affected individuals. For breaches involving fewer than 500 individuals, the covered entity may maintain a log of any breaches and submit the log to the Secretary within 60 days of the end of each calendar year.

HHS notes that contrary state breach notification laws will be preempted by the Interim Final Rule, and covered entities must analyze relevant state laws with respect to the Interim Final Rule in determining whether a state law is contrary to the federal rule and, thus, preempted. Nonetheless, HHS believes that in most cases, a single notification can satisfy both state and federal laws.

Based on the plain language of the statute, the provisions of the Interim Final Rule apply to business associates and covered entities 30 days after publication in the *Federal Register*. By contrast, the plain language of the statute also states that HIPAA penalties do not apply against business associates for violating the security breach provisions until February 17, 2010, but they could be applied immediately for covered entities. Nonetheless, HHS, in the commentary to the Interim Final Rule specifically acknowledged this statutory “ambiguity” and stated that it will exercise its enforcement discretion and not enforce these regulations—against anyone—until 180 days after the publication date (or roughly February 20, 2010).

The practical effect is that covered entities and business associates have some time to prepare their respective organizations before February 20, 2009. However, because the plain language of the Interim Final Rule states that it applies against covered entities 30 days after publication in the *Federal Register* and it can be argued that the Rule applies against business associates as of the same date, covered entities and business associates should begin updating their organizational processes as soon as possible so they can be ready to comply as soon as the Interim Final Rule is enforced.

## FTC’s Health Breach Notification Rule

Pursuant to the requirements of the HITECH Act, the FTC has published the final rule that requires vendors of PHRs and related entities to notify individuals when the security of their identifiable health information is breached (available at <http://edocket.access.gpo.gov/2009/pdf/E9-20142.pdf>). The Health Breach Notification Rule will place considerable obligations on vendors of PHRs and related entities in the event of a security breach. In addition, vendors of PHRs will likely incur significant time and expense to implement measures to secure individually identifiable health information to prevent security breaches.

In large part, the rule follows the security breach notification requirements set forth in the HITECH Act. Following the discovery of a security breach, the rule requires vendors of PHRs and related entities to notify the FTC, each individual whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of the breach, and, in some instances, the media. The FTC defines PHR identifiable health information as “individually identifiable health information” (as defined in HIPAA) and “with respect to individuals, information that is provided by or on behalf of the individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.” The FTC explains that PHR identifiable health information does not include “de-identified” information, as that term is defined in HIPAA, but can include disclosure of credit card information in certain circumstances. The FTC’s definition of “unsecured” references the definition used by HHS in its Interim Final Rule.

A key addition to the final rule from the HITECH Act itself is the FTC’s pronouncement that an unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor or entity that experienced the breach has reliable evidence showing there has not been, or could not reasonably have been, any unauthorized

acquisition of such information. This addition offers at least some opportunity for organizations who have suffered a breach to examine the particular facts involved and then assess whether there was merely an opportunity to access information (which under the FTC's interpretation would not be reportable) versus determining that the information was actually acquired, which would be reportable. For example, if a laptop is stolen in a public place and later recovered, the entity owning the laptop can rebut the presumption that unauthorized acquisition occurred by demonstrating that the files on the laptop were never opened, transferred, *etc.*

Additional requirements set forth in the proposed rule include the following items.

#### WHO MUST COMPLY

Vendors of PHRs and PHR related entities that offer products or services through the website of a vendor of PHRs, offer products or services through the websites of covered entities that offer individuals PHRs, access information in a PHR or send information to a PHR must comply.

Third party service providers that provide services to a vendor of PHRs or to a PHR related entity must notify the appropriate PHR vendor or PHR related entity of a security breach related to such vendor or related entity's customers, and for this reason, vendors of PHRs and PHR related entities must notify third party service providers of their status as vendors of PHR and PHR related entities. Additionally, the contract between the third party service provider and the vendor of PHRs or PHR related entity should specify the individual at the PHR vendor or PHR related entity to whom the third party service provider should provide notice in the event of a security breach.

Note that the FTC regulations apply to non-profit entities and other entities that are not typically regulated by the FTC if such entities are vendors of personal health records or PHR related health entities.

#### TIMELINESS OF NOTIFICATION

Notifications must be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security, unless otherwise directed by a law enforcement official.

#### METHODS OF NOTICE

Notice must be provided in writing by first class mail to the affected individuals or by electronic mail if the individual is given a clear, conspicuous and reasonable opportunity to receive notification by first-class mail and does not exercise that choice. In circumstances where there are 10 or more individuals who cannot be reached after reasonable efforts to make contact, a conspicuous posting on the vendor or related entity's internet home page for a period of 90 days or notice in major print or broadcast (TV or radio) media for 90 days may serve as a substitute form of notice. If the breach has affected the unsecured PHR identifiable health information of 500 or more residents of a state or other jurisdiction (such as a city or town), notice must also be provided to prominent media outlets following the discovery of a breach. The vendor or related entity must also notify the FTC on the FTC-approved form within 10 days following the discovery of a breach of security.

#### CONTENTS OF NOTICE:

Notice of a security breach must be in plain language and must include a brief description of what happened; the types of unsecured PHR identifiable health information that were involved; and actions performed by the entity to investigate the breach, to mitigate losses and to protect against further breaches. Notices should also include recommended steps individuals should take to protect themselves from potential harm and contact procedures for individuals to ask questions or learn additional information.

## LOGGING BREACHES

If a vendor of PHRs or a PHR related entity discovers a breach involving fewer than 500 individuals, then the entity may maintain a log of such breaches and submit the log annually to the FTC no later than 60 days following the end of a calendar year, documenting breaches for such calendar year.

## ENFORCEMENT

A violation of the proposed rule will be treated as an unfair or deceptive act or practice in violation of the Federal Trade Commission Act.

## HEALTH BREACH NOTIFICATION RULE

Additionally, the FTC provided important clarifications to its interpretation of the Health Breach Notification Rule:

- *“In a personal health record”*: The FTC reads “in a personal health record” to include both data at rest and data in motion.
- *Inadvertent Access by Employees*: If an employee of a vendor of PHRs or PHR related entity inadvertently accesses PHR identifiable information, no breach notification is required if the employee follows the entity’s policies by reporting the instance to his or her supervisor and affirming that he or she did not read or share the data that was accessed, and the entity “conducts a reasonable investigation to corroborate the employee’s version of the events.”
- *Limited Data Sets*: The FTC declined to state that limited data sets and “redacted, truncated, obfuscated, or otherwise pseudonymized” are not PHR identifiable health information because the risk of re-identification is too great.
- *When a breach is “discovered”*: Breaches are treated as “discovered” on the “first day on which such breach is known or reasonably should have been known to the vendor of personal health records, PHR related entity, or third party service provider, respectively,” and an entity is deemed to have “knowledge of a breach if such breach is known, or reasonably should have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent” of such entity.
- *The 60-day Period*: As with the HHS Interim Final Rule, notice must be sent no later than 60 days of discovery of a breach, but if the entity could reasonably conclude its investigation and send notice prior to 60 days, it may not be appropriate to allow the entire time to elapse. Additionally, FTC, like HHS, clarified that the purpose of the 60 days is to give entities time to conduct an appropriate investigation of the breach, and the 60-day period does not start when the investigation is complete.

The federal FTC requirements supersede any contrary state laws; however, the FTC regulations do not preempt state laws that impose additional breach notification requirements (for example, state laws requiring that breach notices contain contract information for consumer reporting agencies or advice on monitoring credit reports). Nonetheless, FTC believes that this will not require entities to send multiple notices to comply with both federal and state law.

The text of the final rule is available from the FTC’s website at <http://www.ftc.gov/os/2009/08/R911002hbn.pdf>. The final rule will be effective on September 24, 2009, and full compliance will be required February 21, 2010, as the FTC has stated that it will use its enforcement discretion to refrain from bringing enforcement actions before that time. Therefore, vendors of PHRs, PHR related entities and their third party service providers should begin immediately to implement processes and procedures that will allow for timely notification of security breaches under the final rule. In addition, they should obtain and maintain reasonable security measures to assist them in discovering breaches in a timely fashion.

## Implications of the HHS Interim Final Rule and the FTC Health Breach Notification Rule

### DUAL NOTIFICATION/OVERLAPPING REGULATIONS:

The FTC drafted its regulations in order to prevent overlap with the HHS regulations because many commenters were concerned that the two parallel sets of regulations would cause consumers to receive dual notifications of security breaches. Specifically, the FTC regulations do not apply to HIPAA covered entities acting in their capacities as covered entities. However, if, for example, a physician creates a PHR in his or her personal capacity as part of a start-up business venture, then the FTC regulations (rather than the HHS regulations) would apply to the business venture. Additionally, in certain circumstances vendors of PHRs may provide notice directly to consumers even when they serve as the business associates of a covered entity. If a vendor of PHRs provides notice on behalf of a covered entity, has dealt directly with the individuals who receive the notice in managing their PHR accounts and provides notice on behalf of the covered entity at the same time that it provides FTC-required notice to its other customers, then the FTC will deem compliance with the HHS regulations as compliance with the FTC regulations as well.

### SPECIAL RECORDKEEPING FOR PHR VENDORS WHO ARE ALSO BUSINESS ASSOCIATES

In order to fulfill its separate obligations under both sets of regulations, the FTC states that a vendor of PHRs should maintain a list of all of its own customers along with a separate list for its business associates' customers. Vendors of PHRs must also maintain and update regularly lists tracking which customers belong with which covered entity.

### RISK ASSESSMENTS/INVESTIGATIONS

The risk assessments and investigations contemplated by both sets of regulations will involve both factual and legal components and will consume time and resources for the entity involved. Therefore, it is important to prepare for these undertakings before a security breach occurs by contacting your legal counsel and business consultants, who can assist you in developing a plan for these types of risk assessments and investigations.

The HHS guidance carries with it critically important implications for HIPAA covered entities and their business associates in that each must look deeply into their current security infrastructures—covered entities because they are currently covered by HIPAA, and business associates because they are already contractually committed to notify their covered entity customers of breaches, and will, as of February 17, 2010, be directly subject to HIPAA's civil and criminal penalties. For many of these organizations, particularly those smaller providers and vendors, the concept of encryption and the associated NIST standards are likely to be foreign. These standards are complex and costly, and will involve a great deal of IT management time as well as training of users in order to meet even the spirit of the guidance. Nevertheless, taking steps now to begin implementing the proper encryption components to one's operations should prove to be a wise investment when a laptop, for example, is lost or stolen. Similarly, the FTC's proposed regulations offers some useful commentary regarding the difference between situations where information could have been accessed contrasting that to situations in which it was actually acquired.

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

**Stephen W. Bernstein:** +1 617 535 4062 sbernstein@mwe.com

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

**Heidi Y. Echols:** +1 312 984 7559 hechols@mwe.com

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

**Erin Davis Shedd:** +1 312 984 2723 edavishedd@mwe.com

For more information about McDermott Will & Emery visit [www.mwe.com](http://www.mwe.com).

The material in this publication may not be reproduced, in whole or part without acknowledgement of its source and copyright. "Regulatory Update: HITECH's Security Breach Notification Requirements" is intended to provide information of general interest in a summary manner and should not be construed as individual legal advice. Readers should consult with their McDermott Will & Emery lawyer or other professional counsel before acting on the information contained in this publication.

© 2009 McDermott Will & Emery. The following legal entities are collectively referred to as "McDermott Will & Emery," "McDermott" or "the Firm": McDermott Will & Emery LLP, McDermott Will & Emery/Stamford LLP, McDermott Will & Emery Rechtsanwälte Steuerberater LLP, MWE Steuerberatungsgesellschaft mbH, McDermott Will & Emery Studio Legale Associato and McDermott Will & Emery UK LLP. McDermott Will & Emery has a strategic alliance with MWE China Law Offices, a separate law firm. These entities coordinate their activities through service agreements. This communication may be considered attorney advertising. Previous results are not a guarantee of future outcome.