

October 2009

## **Notification Requirement for Security Breaches of Protected Health Information**

**The Department of Health and Human Services ("HHS") published regulations on August 24, 2009, requiring HIPAA covered entities and their business associates to notify affected individuals as well as HHS, and in some cases the media, of any security breaches involving Protected Health Information ("PHI"). This Alert provides an overview of these new interim final regulations, which took effect on September 23, 2009.**

### **Background: HITECH Act Security Breach Notification Requirement**

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (commonly referred to as "ARRA" or the "Stimulus Bill"), which includes the Health Information Technology for Economic and Clinical Health Act (or the "HITECH Act" for short). The HITECH Act provides incentives for the use of electronic health records and expands the obligations of covered entities and business associates under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and related Privacy and Security Rules to protect the confidentiality and security of PHI.<sup>[1]</sup>

The security breach provisions of the HITECH Act require covered entities and business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI to provide notification upon discovering a "breach" of unsecured PHI. For purposes of this notification requirement, a "breach" is generally defined as the unauthorized acquisition, access, use or disclosure of unsecured PHI.

The HITECH Act required the Secretary of HHS to publish interim final regulations on notification of breach within 180 days after enactment, and provided that the breach notification requirement will take effect 30 days after the publication of these interim final regulations. HHS published interim final breach notification regulations on its website August 19, 2009, prior to publication in the Federal Register on August 24, 2009.

### **Who is Subject to the Security Breach Rule?**

The obligation to report security breaches applies to HIPAA covered entities, including a broad range of health plans, health care providers and health care clearinghouses, and to business associates. In general, a business associate is a person or entity (other than a member of the covered entity's workforce) that, on behalf of a covered entity, performs any activity involving the use or disclosure of PHI, such as the performance of financial, legal, actuarial, accounting, consulting, data aggregation, management, administrative or accreditation services.

This Alert focuses on the security breach obligations of covered entities and their business associates under the HITECH Act and the security breach rule published by HHS. Vendors of Personal Health Records (PHRs) and their service providers are subject to similar security breach rules issued by the Federal Trade Commission (FTC). In some situations, an entity may be subject to both the HHS and FTC breach notification rules. For example, a vendor of PHRs to both a HIPAA covered entity and the public may be subject to both the FTC security breach rules and the HHS breach notification rules.

### **Unsecured PHI Subject to the Security Breach Notification Requirements**

The obligation to provide notice of a security breach applies only to security breaches of "unsecured" PHI. Protected health information (PHI) is individually identifiable health information held or transmitted by a covered entity or its business associates, in any form or media.

The HITECH Act defines "unsecured protected health information" as PHI that is not secured through the use of a technology or methodology specified in guidelines issued by the Secretary of HHS as rendering PHI "unusable, unreadable or indecipherable to unauthorized individuals." On April 17, 2009, HHS issued guidance identifying encryption and destruction as the two methods for securing PHI and describing standards for both methods.

In its preamble to the August 24, 2009 rule, HHS noted some confusion about its April guidance and clarified several issues. In particular:

- A covered entity is not required to encrypt PHI, but encryption in accordance with the guidance would relieve a covered entity of the breach notification requirement because the encrypted PHI is unusable, unreadable or indecipherable to unauthorized individuals and is therefore not "unsecured;"
- Even though access controls may have value by preventing breaches of unsecured PHI, if access controls are compromised, the incident may require notification unless encryption standards are satisfied;
- Encryption keys must be stored on a separate device from the encrypted data in order to satisfy the encryption standard; and
- Redaction of paper records is not a recognized alternative to destruction or encryption as a means to secure PHI. HHS recognized, however, that in some cases the notification requirement may be avoided with respect to redacted information if the redaction successfully de-identifies all PHI, or if the unredacted information does not compromise the security or privacy of the information.

## **How to Determine Whether a Reportable Breach Occurred**

Upon becoming aware of an incident involving the security of PHI, the covered entity or business associate will need to promptly determine whether the incident triggers the obligation to notify the affected individuals, HHS and in some cases the media. The regulations define "breach" as "the acquisition, access, use or disclosure of protected health information in a manner not permitted" under the HIPAA Privacy Rule "which compromises the security or privacy of the protected health information." Under the regulations, a covered entity or business associate will need to follow a three step process in determining whether an incident is deemed to be a breach triggering the notification obligation.

The first step is to determine whether there has been a use or disclosure that is not permitted under the HIPAA Privacy Rule. HHS noted that a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and that occurs despite reasonable safeguards and proper minimum necessary procedures would not violate the Privacy Rule and therefore would not be deemed to be a breach. A violation of administrative requirements, such as lack of reasonable safeguards or training, would not of itself be a breach, but may lead to impermissible uses or disclosures that may be deemed to be breaches.

The second step is to perform a risk assessment to determine and document whether the impermissible use or disclosure compromises the security or privacy of the PHI by creating a significant risk of harm to the individual. The regulations specifically reference financial and reputational harm, but also include a general reference to "other harm to the individual." This risk assessment involves analysis of who improperly used or received PHI and the type and amount of PHI involved, as well as other factors such as steps to mitigate the harm and whether the PHI is returned prior to being accessed. For example, disclosure to someone who has no obligation to maintain the privacy and security of PHI would typically pose a higher degree of risk than disclosure to a HIPAA covered entity that is obligated to protect the confidentiality of PHI or to someone who provides satisfactory assurances that the PHI will be destroyed or will not be used or disclosed. HHS noted that disclosure limited to the name of a hospital patient will not necessarily pose a significant risk (even though the disclosure may violate the Privacy Rule), but that the risk of harm would be higher if the disclosure reveals the type of services, the specialized nature of the health care facility, or information posing identity theft concerns. If the disclosure is of a limited data set, the risk assessment would need to consider whether the risk of identifying the individual is so small that the disclosure does not pose significant risk of harm to the individual. This second step will typically require a fact-intensive analysis to determine whether the risk of harm is significant, and in many cases, may not generate a bright line result.

The third step in the breach analysis is to determine whether the incident falls within any of the following three exceptions that will not trigger the notification obligation:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the covered entity or of a business associate, if the acquisition, access or use was made in good faith, was within the scope of authority, and does not result in further use or disclosure in violation of the Privacy Rule;
- Inadvertent disclosure between persons who are authorized to access PHI within the same covered entity, a business associate of the covered entity, or an organized health care arrangement (for example, a hospital and physicians on its medical staff), if the PHI is not further used or disclosed in violation of the Privacy Rule; or
- Disclosures where the covered entity or business associate has a good faith belief that the unauthorized recipient of the PHI would not reasonably be able to retain the PHI.

## **Notification Obligations of Covered Entities**

Upon discovery of a breach of unsecured PHI, the covered entity will be required to notify each individual whose unsecured PHI has been (or is reasonably believed by the covered entity to have been) used or disclosed as a result of the security breach. The notification must be made "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach," and must satisfy requirements relating to content, plain language and logistics.

The clock starts ticking for purposes of the notification deadline when the breach is deemed to be "discovered." The

regulations provide that a breach will be deemed to be discovered on the earlier of the date the breach first becomes known to the covered entity or the date the breach would have been known if the covered entity had exercised reasonable diligence. A covered entity is regarded as having knowledge of a breach if and when the breach becomes known, or in the exercise of reasonable diligence would have been known, to any workforce member or agent of the covered entity, other than the person committing the breach. It is therefore imperative for covered entities to train their personnel to promptly identify and report potential breaches to appropriate compliance personnel for review.

The regulations set forth additional reporting obligations to HHS and in some cases to the media. If a breach involves more than 500 residents of any state, the covered entity will be required to notify prominent media outlets in the state without unreasonable delay and in no case later than 60 days after discovery of the breach.

All breaches will be required to be reported to HHS, with the timing based on whether the breach involves 500 or more individuals. If a breach involves fewer than 500 individuals, the covered entity will be required to maintain a log or other documentation of breaches and to notify HHS within 60 days after the end of the calendar year. In the case of a breach involving 500 or more individuals, the report to HHS must be made without unreasonable delay and in no case later than 60 days after discovery of the breach.

Notification is generally required to be by first-class mail, although the notice may be by e-mail if the individual has agreed to electronic notice. The regulations also allow notification to be provided by alternative means, such as telephone, the covered entity's website or media, if insufficient or out-of-date contact information precludes notice by mail or e-mail. A covered entity may supplement written notice with notice by telephone or other means in circumstances that are urgent due to possible imminent misuse of unsecured PHI.

The regulations provide for a delay in providing notification if a law enforcement official states that notice would impede a criminal investigation or cause damage to national security.

## **Business Associates**

A business associate who discovers a breach will be required to notify the covered entity without unreasonable delay and in no case later than 60 days after discovery. The discovery standard for business associates is similar to the standard for covered entities.

The legal relationship between a covered entity and its business associates may have an impact on when the clock starts ticking on a covered entity's obligation to provide notice. A business associate's discovery of a breach will be imputed to the covered entity if the business associate is deemed to be an agent of a covered entity, in which case the covered entity's notice period would begin when the business associate discovers the breach, rather than when the business associate notifies the covered entity of the breach. On the other hand, if the business associate is an independent contractor, and not an agent, the notice period for the covered entity to report a breach discovered by the business associate would begin to run when the business associate notifies the covered entity of the breach unless the covered entity previously discovered the breach.

There is some uncertainty regarding whether the HITECH Act and the security breach regulations require existing HIPAA business associate agreements to be amended to reflect the security breach regulations. A cautious approach would be to amend existing and template business associate agreements to incorporate appropriate security breach safeguards. Moreover, it will often be in the interest of covered entities (and in some cases, business associates) to include specific security breach provisions in their business associate agreements, such as deadlines for reporting security breaches to the covered entity, description of information to be provided in the report, and any obligations of the business associate to satisfy encryption standards or to provide security breach notifications on behalf of the covered entity.

Business associates will need to take appropriate steps to ensure that they can satisfy their duties under business associate agreements and under the security breach regulations. For example, to the extent that a business associate engages a subcontractor to perform the business associate's PHI-related functions, the subcontractor should be required to promptly notify the business associate of any security breaches, and could be required to implement appropriate policies and procedures.

## **Effective Date**

The interim security breach rule took effect on September 23, 2009. HHS acknowledged that it will take time for covered entities and business associates to implement policies, procedures and systems needed in order to comply with the security regulations. HHS therefore stated that it will use its enforcement discretion to not impose sanctions under the security rule for breaches that are discovered prior to February 22, 2010.

While this five month delay in enforcement provides some measure of relief, covered entities and business associates should be wary of delaying compliance, as they could face exposure from a variety of other fronts beginning on the September 23, 2009 effective date. In particular, covered entities and business associates could be subject to lawsuits filed by patients based on security breaches after the security breach rule becomes effective, or perhaps under state laws imposing similar security breach obligations. Moreover, the American Medical Association adopted

guidelines in June 2009, calling for physicians to inform their patients of security breaches and respond to security breaches.

## Comment Period

HHS is accepting comments until October 23, 2009. In light of the interim nature of the security breach rule, it is likely that some changes will eventually be made. Unless and until amended, however, the interim final regulations should be followed.

## What Should Covered Entities and Business Associates Do Now?

Covered entities and business associates should promptly take steps to minimize the likelihood and severity of security breaches and detect and respond to potential security breaches, including:

- Periodically review the security breach regulations as well as any state laws or regulations relating to security breaches;
- Train and educate personnel to promptly report potential breaches to appropriate management or compliance personnel within the covered entity or business associate;
- Incorporate security breach provisions into HIPAA business associate agreements, including amendments to existing business associate agreements;
- Review and update policies, procedures, systems and other safeguards to address security breaches and related issues;
- Update policies, procedures and systems again when additional or updated HITECH Act or HIPAA regulations are issued (additional regulations are expected to be issued later this year);
- Promptly investigate any potential breaches to determine whether security breach notification obligations are triggered, and document this analysis;
- Notify the affected individuals (or, in the case of a business associate, the covered entity) without unreasonable delay, and in any event within 60 days after discovery, and also provide notification to HHS and the media to the extent required;
- Document any security breach notifications, as well as any determination that notice is not required, keeping in mind that the covered entity or business associate will have the burden of proof to show that all required security breach notifications were provided or that the use or disclosure in question was not a breach triggering the notification requirement.

\* \* \*

To find out more about how to comply with the HITECH Act or the security breach regulations, please contact:

**Rick L. Hindmand**, 312.280.0111 rhindmand@mcdonaldhopkins.com

**John T. Mulligan**, 216.348.5435 jmulligan@mcdonaldhopkins.com

**Rachel Solomon**, 312.280.0111 rsolomon@mcdonaldhopkins.com

**Jane Pine Wood**, 508.385.5227 jwood@mcdonaldhopkins.com

---

[1] For a general discussion of the HIPAA provisions of the HITECH Act, please click here to see our June, 2009, Alert.

## Healthcare Practice Group

McDonald Hopkins has a large and diverse healthcare practice, which is national in scope. The firm represents a wide variety of healthcare providers, facilities, vendors, technology companies and associations. Our diverse experience enables us to give our clients a unique perspective on the issues that may confront them in the rapidly evolving healthcare environment.



**600 Superior Avenue, East, Suite 2100, Cleveland, Ohio 44114**

**Chicago | Cleveland | Columbus | Detroit | West Palm Beach**

To ensure compliance with requirements imposed by the Internal Revenue Service, we inform you that any tax advice contained in this communication (including any attachments), was not intended or written to be used, and cannot be used, by any taxpayer for the purpose of (1) avoiding any penalties under the Internal Revenue Code or (2) promoting, marketing or recommending to another party any transaction matter addressed herein.

© 2009 McDonald Hopkins LLC All Rights Reserved

This Publication is designed to provide current information for our clients, friends and their advisers regarding important legal developments. The foregoing discussion is general information rather than specific legal advice. Because it is necessary to apply legal principles to specific facts, always consult your legal adviser before using this discussion as a basis for a specific action.