

## **New HIPAA Breach Notification Regulations Issued by HHS under the HITECH Act**

**September 2, 2009**

On August 24, the Department of Health and Human Services (HHS) published regulations (the Breach Notification Regulations or Regulations) that impose significant new breach notification obligations upon “covered entities” and “business associates” subject to the Health Insurance Portability and Accountability Act of 1996 and related regulations (the HIPAA Regulations or HIPAA).

The Health Information Technology for Economic and Clinical Health Act (the HITECH Act), which is part of the American Recovery and Reinvestment Act of 2009 (ARRA) enacted on February 17, 2009, contains significant amendments to the HIPAA Regulations. Among the most noteworthy features of the HITECH Act is a requirement that, in certain instances, covered entities must notify affected individuals, the media, and/or the Secretary of HHS (the Secretary) in the event of a breach of Unsecured Protected Health Information (unsecured PHI). Pursuant to the Breach Notification Regulations, covered entities are required to report breaches that are discovered on or after September 23, 2009.

### **The General Rule**

Simply stated, the Breach Notification Regulations require covered entities to provide notification to affected individuals, the media, and/or the Secretary following the “discovery” of a “breach” of “unsecured PHI.” Each of these three defined terms adds another layer of complexity to the analysis of whether a covered entity or business associate has a notification obligation in a particular situation.

### **What Is Unsecured PHI?**

The Breach Notification Regulations only apply to breaches involving “unsecured PHI,” which is PHI “that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance.” The Breach Notification Regulations, which essentially adopt and clarify the HHS guidance published on April 27, 2009 regarding the meaning of unsecured PHI, specify that encryption and destruction are the core methodologies available to secure PHI. Notably, the Regulations specify that access controls and redaction, while valid methods to protect and maintain the privacy of PHI, are not methodologies or technologies that “secure” PHI. For example, if PHI stored on a laptop is password-protected, but not encrypted, then the PHI will be considered “unsecured.” In addition, the Regulations clarify that a

limited data set (which is created by removing 16 identifiers from PHI) is not a method by which PHI may be “secured.”

The Regulations set forth encryption standards for electronic PHI that is “in motion,” “at rest,” and “in use.” In general, information may be “secured” by encryption through “the use of an algorithmic process to transfer data into a form in which there is a low probability of assigning meaning without use of a confidential process or key,” as long as the confidential process or key is not breached. To ensure that the confidential process or key is not breached, the decryption tools need to be stored at a location (or on a device) that is separate from the encrypted data. More specific information about acceptable encryption methodologies and technologies is contained in National Institute of Standards and Technology (NIST) publications, which are identified in the Breach Notification Regulations.

To meet the Regulation’s data destruction requirements, hardcopy media containing PHI (such as paper or film) must be shredded or otherwise destroyed in a manner that ensures it cannot be read or reconstructed. Electronic media containing PHI must be destroyed in accordance with NIST Special Publication, 800-88, *Guidelines for Media Sanitization*, so that the PHI cannot be retrieved.

HHS acknowledges that the technologies and methodologies approved by the Secretary serve as a functional safe harbor with respect to the breach notification requirements. If PHI is “secured” as set forth in the Regulations, then, in the event of a breach, the covered entity will not be required to notify affected individuals. HHS emphasizes, however, that its guidance regarding unsecured PHI does not impose a requirement that covered entities encrypt all PHI; under the HIPAA security regulations (the Security Rule), encryption remains an “addressable” (not “required”) implementation specification.

### **When Is Unsecured PHI Breached?**

Notification is only required when the privacy of unsecured PHI has been “breached.” Under the Breach Notification Regulations, a breach occurs when there is unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of that information.

To determine if a breach has occurred, the covered entity or business associate must apply a three-step analysis in which it must determine the following:

1. Whether there has been an impermissible use or disclosure of PHI under the HIPAA privacy regulations (the Privacy Rule)
2. Whether such impermissible use or disclosure compromises the security or privacy of the PHI, which occurs if there is a **“significant risk of financial, reputational or other harm to the individual.”** To determine if this “significant risk of harm” standard has been met, the covered entity or business associate must perform and document a fact-specific risk assessment
3. Whether the incident falls within one of the following three limited exceptions to the definition of breach:
  - (i) Any unintentional access, use, or disclosure of PHI by a covered entity’s or business associate’s workforce member or person acting under the authority

thereof, if such access was in good faith, within that person's scope of authority, and did not result in further impermissible use or disclosure of the PHI

- (ii) Any inadvertent disclosure by a person who is authorized to have access to such PHI to another authorized person at the same covered entity or business associate, or organized healthcare arrangement in which the covered entity participates, and the PHI disclosed is not further used or disclosed in an impermissible manner
- (iii) Disclosure of the PHI where the covered entity or business associate has a good faith belief that the unauthorized person who received the PHI would not reasonably have been able to retain the PHI

The above-described "significant risk of harm" standard is perhaps the most important new development introduced in the Breach Notification Regulations because it qualifies a covered entity's obligation to notify individuals of a breach. Prior to introduction of the "significant risk of harm" standard, a covered entity might have been obligated to issue notices of a breach even if it had effectively mitigated any harm that might have resulted from the breach.

The covered entity or business associate bears the burden of proof regarding whether a breach has occurred. Therefore, it is important that covered entities and business associates formalize their risk assessment processes and procedures, and document their breach determinations and the considerations supporting those determinations.

### **When Is the Breach Discovered?**

A breach is treated as "discovered" on "the first day the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity." A covered entity is deemed to have knowledge if the breach is known (or would have been known by the exercise of reasonable diligence) to any workforce member or agent, except to the person who committed the breach. The date of discovery is critical because that date starts the clock for the time period to issue notification of the breach.

Due to the "reasonable diligence" standard, it is important that covered entities establish policies and procedures to ensure the discovery of such breaches, including making sure that workforce members and agents are adequately trained.

### **The Notification Procedures**

When a breach of unsecured PHI is discovered, the covered entity has the following notification obligations:

#### *Notice to Individuals*

Individuals whose unsecured PHI may have been breached are to be notified, as soon as reasonably possible, and in no case later than 60 calendar days after the breach is discovered (not 60 days after an

investigation of the breach is completed). Written notice should be sent to individuals by first-class mail to their last known address, or by email if the individual has agreed to accept electronic notice.

The Regulations also contain special notification rules related to (a) notification to personal representatives, (b) substitute notice if a covered entity becomes aware that it has insufficient or out-of-date address information, and (c) urgent notice if the covered entity believes there is a possibility of imminent misuse of the unsecured PHI.

The notice must be written in plain language, and it must contain (a) a brief description of what happened; (b) a description of the type of unsecured PHI involved in the breach; (c) steps that impacted individuals should take to protect themselves from potential harm resulting from the breach; (d) a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and protect against further breaches; and (e) contact information for individuals to use if they have questions or need additional information.

### ***Notice to Media***

If the breach involves (or is reasonably believed to have involved) more than 500 residents in a state or jurisdiction, prominent media outlets serving that state or jurisdiction must be notified. The notice must be provided in the same time frame and must contain the same content as the notice to the affected individuals. Notice to the media is a supplement to the individual notice; it is not a substitute for such notice.

### ***Notice to the Secretary***

Covered entities are required to notify the Secretary of all discovered breaches of unsecured PHI. If the breach involves 500 or more individuals, the Secretary must be provided notice at the same time as the affected individuals. In addition, if a breach involves more than 500 individuals, the Secretary will post the name of the breaching covered entity on its website. For breaches that involve fewer than 500 individuals, the covered entity may notify the Secretary by providing an annual log, which is due no later than 60 days after the end of each calendar year. HHS will be posting instructions on its website about how to submit these two forms of notice.

### ***Business Associates' Notification Obligations***

In general, a business associate is required to notify the covered entity of a breach without unreasonable delay, but in no case later than 60 days following discovery of the breach, and the covered entity is then required to provide the requisite notice to the individuals, media, and/or HHS.

However, for practical purposes, business associate agreements may need to be amended to expand upon the business associate's limited notification obligations outlined above. Such amendments may be necessary due to the following reasons:

- (1) If the business associate is an agent (rather than an independent contractor) of the covered entity, the business associate's discovery of the breach will be imputed to the covered entity, which means the covered entity's 60-day period to notify individuals will run concurrently with the business associate's 60-day period to inform the covered entity of

the breach. It follows that, if the parties plan for the business associate to notify the covered entity and the covered entity to notify the individuals, the business associate agreement may need to be amended to reflect a shorter notification time frame by the business associate.

- (2) In some instances, the business associate will be in a better position to notify the affected individuals of the breach. In such cases, the business associate agreement should be amended to shift the notification obligation to the business associate.

Further, because these Regulations are effective this month, it makes sense for covered entities to confirm with their business associates as to whether they intend to “secure” PHI in accordance with these Regulations.

### **Additional Administrative Requirements**

In addition to the notification obligations described above, the Breach Notification Regulations impose the following related administrative obligations on covered entities, requiring them to:

- (1) Revise their policies and procedures to account for the notification requirements
- (2) Train their workforce members to secure PHI and to promptly notify the covered entity or business associate if the privacy or security of unsecured PHI has been breached
- (3) Sanction workforce members who violate the notification requirements
- (4) Permit individuals to file complaints if they believe the notification requirements have been violated
- (5) Refrain from intimidating or retaliating against individuals who seek to enforce their rights related to the notification requirements, and refrain from requiring individuals to waive their rights under the Regulations as a condition of treatment, payment or health plan participation
- (6) Retain documentation related to the notification requirements for six years

In addition, as noted above, business associate agreements may need to be revisited to specify whether any portion of the notification obligation will be assumed by the business associate.

### **The Effective Date**

The Breach Notification Regulations are effective 30 days from August 24, 2009 (*the date the Regulations were published in the Federal Register*), or September 23, 2009. However, HHS acknowledges that 30 days is a short time period to implement the procedures and mechanisms necessary to comply with the Regulations. HHS has thus decided to use its enforcement discretion to not impose sanctions for failure to provide the requisite breach notifications between August 24, 2009 and February 22, 2010 (*180 days later*). During this six-month period, covered entities are expected to comply with the Breach Notification Regulations, but HHS will apply technical assistance and voluntary corrective action to achieve compliance, rather than punitive measures.

Despite the 180-day enforcement grace period granted by HHS, covered entities and business associates should not delay in developing and implementing new policies, procedures, and training to ensure compliance with the Breach Notification Regulations. These new compliance measures will not only aid organizations in complying with Breach Notification Regulations as of the September 23, 2009 compliance date, but will also facilitate compliance with state security breach notification laws and mitigate liability risks associated with privacy- and security-related lawsuits arising under state common law, to the extent such state laws are applicable.

If you would like more information on any of the issues discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

### **Chicago**

David Ackerman	312.324.1170	<a href="mailto:dackerman@morganlewis.com">dackerman@morganlewis.com</a>
Andy R. Anderson	312.324.1177	<a href="mailto:aanderson@morganlewis.com">aanderson@morganlewis.com</a>
Brian D. Hector	312.324.1160	<a href="mailto:bhector@morganlewis.com">bhector@morganlewis.com</a>

### **Dallas**

Riva T. Johnson	214.466.4107	<a href="mailto:riva.johnson@morganlewis.com">riva.johnson@morganlewis.com</a>
John A. Kober	214.466.4105	<a href="mailto:jkober@morganlewis.com">jkober@morganlewis.com</a>
Heath Miller	214.466.4118	<a href="mailto:hmiller@morganlewis.com">hmiller@morganlewis.com</a>
Erin Turley	214.466.4108	<a href="mailto:eturley@morganlewis.com">eturley@morganlewis.com</a>

### **New York**

Craig A. Bitman	212.309.7190	<a href="mailto:cbitman@morganlewis.com">cbitman@morganlewis.com</a>
Gary S. Rothstein	212.309.6360	<a href="mailto:grothstein@morganlewis.com">grothstein@morganlewis.com</a>

### **Palo Alto**

S. James DiBernardo	650.843.7560	<a href="mailto:jdibernardo@morganlewis.com">jdibernardo@morganlewis.com</a>
Zaitun Poonja	650.843.7540	<a href="mailto:zpoonja@morganlewis.com">zpoonja@morganlewis.com</a>

### **Pittsburgh**

Lisa H. Barton	412.560.3375	<a href="mailto:lbarton@morganlewis.com">lbarton@morganlewis.com</a>
John G. Ferreira	412.560.3350	<a href="mailto:jferreira@morganlewis.com">jferreira@morganlewis.com</a>
Lauren Bradbury Licastro	412.560.3383	<a href="mailto:llicastro@morganlewis.com">llicastro@morganlewis.com</a>
R. Randall Tracht	412.560.3352	<a href="mailto:rtracht@morganlewis.com">rtracht@morganlewis.com</a>

### **Philadelphia**

Robert L. Abramowitz	215.963.4811	<a href="mailto:rabramowitz@morganlewis.com">rabramowitz@morganlewis.com</a>
I. Lee Falk	215.963.5616	<a href="mailto:ilfalk@morganlewis.com">ilfalk@morganlewis.com</a>
Amy Pocino Kelly	215.963.5042	<a href="mailto:akelly@morganlewis.com">akelly@morganlewis.com</a>
Robert J. Lichtenstein	215.963.5726	<a href="mailto:rlichtenstein@morganlewis.com">rlichtenstein@morganlewis.com</a>
Georgina O'Hara	215.963.5188	<a href="mailto:go'hara@morganlewis.com">go'hara@morganlewis.com</a>
Joseph E. Ronan, Jr.	215.963.5793	<a href="mailto:jronan@morganlewis.com">jronan@morganlewis.com</a>
Steven D. Spencer	215.963.5714	<a href="mailto:sspencer@morganlewis.com">sspencer@morganlewis.com</a>
Mims Maynard Zabriskie	215.963.5036	<a href="mailto:mzabriskie@morganlewis.com">mzabriskie@morganlewis.com</a>
David B. Zelikoff	215.963.5360	<a href="mailto:dzelikoff@morganlewis.com">dzelikoff@morganlewis.com</a>

**San Francisco**

Reece Hirsch 415.442.1422 [rhirsch@morganlewis.com](mailto:rhirsch@morganlewis.com)

**Washington, D.C.**

Jessica R. Bernanke 202.739.5447 [jbernanke@morganlewis.com](mailto:jbernanke@morganlewis.com)  
Althea R. Day 202.739.5366 [aday@morganlewis.com](mailto:aday@morganlewis.com)  
Benjamin I. Delancy 202.739.5608 [bdelancy@morganlewis.com](mailto:bdelancy@morganlewis.com)  
David R. Fuller 202.739.5990 [dfuller@morganlewis.com](mailto:dfuller@morganlewis.com)  
Mary B. (Handy) Hevener 202.739.5982 [mhevener@morganlewis.com](mailto:mhevener@morganlewis.com)  
Dean R. Morley 202.739.5989 [dmorley@morganlewis.com](mailto:dmorley@morganlewis.com)  
Gregory L. Needles 202.739.5448 [gneedles@morganlewis.com](mailto:gneedles@morganlewis.com)

**About Morgan, Lewis & Bockius LLP**

Morgan Lewis is an international law firm with more than 1,400 lawyers in 22 offices located in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Minneapolis, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, and Washington, D.C. For more information about Morgan Lewis, please visit [www.morganlewis.com](http://www.morganlewis.com).

This LawFlash is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered Attorney Advertising in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes.

© 2009 Morgan, Lewis & Bockius LLP. All Rights Reserved.