THE NEW HIPAA "BREACH NOTIFICATION" RULE

Scott Warrick, JD, MLHR, CEQC, SPHR

Scott Warrick's Consulting & Employment Law Services

(614) 367-0842: Office ♣ (614) 738-8317: Cell

www.scottwarrick.com

I. THE NEW HIPAA "BREACH NOTIFICATION" RULE

The Health Information Technology for Economic and Clinical Health ("HITECH") Act was signed into law on February 17, 2008 as part of the American Recovery and Reinvestment Act of 2009 (H.R. 1). The American Recovery and Reinvestment Act of 2009 ("the Act") made several changes to the HIPAA privacy rules—including adding a requirement for notice to affected individuals of any breach of unsecured protected health information. On August 24, 2009, the Department of Health and Human Services (HHS) published an interim final rule (the "Rule") that lays out the specific steps that HIPAA-covered entities and their business associates must take.

Among other important aspects, the HITECH Act expands the scope and enforcement power of the Health Insurance Portability and Accountability Act (HIPAA), with greater penalties for non-compliance.

HHS has stated that while it expects covered entities to comply with this Rule as of September 23, 2009, it will not impose sanctions for failure to provide the required notifications for breaches discovered through February 22, 2010. Instead, during such period it will work with covered entities to achieve compliance through technical assistance and voluntary corrective action.

Privacy and Security Regulations

HIPAA previously required that "covered entities" enter into contracts or "business associate agreements" (BAAs) with non-covered entities if those transactions involved the exchange of protected health information (PHI). The BAAs required the entities that do work on behalf of providers and insurers to use appropriate safeguards for the PHI they receive from the covered entities. The BAAs also set forth permitted uses and disclosures for the PHI. Prior to HITECH, business associates were not directly subject to either HIPAA or direct government enforcement action.

Business associates must now comply directly with the administrative safeguards, physical safeguards, policies and procedures and documentation requirements of HIPAA. Business associates also must comply with the HIPAA Privacy Rule provisions that would otherwise be applicable to them through the BAAs and any changes to the Privacy Rules (whether or not those changes are covered by the

BAAs). Business associates can now be subject to enforcement by federal or state officials for any failure to comply with HIPAA (as amended by HITECH).

Summary of New Rule

A two-part inquiry is applied for determining if notification is required:

1. Does it qualify as a "breach" and

2. Was the PHI protected by encrypted technology?

No notification to individuals is required if the breached information was covered by an encryption approved by the U.S. Department of Health and Human Services (HHS) *i.e.*, the information has been rendered "unusable, unreadable or in-decipherable to unauthorized individuals," using technology or methodology approved by HHS.

NOTE: The Rule defines a "breach," subject to exceptions discussed below, as the unauthorized acquisition, access, use, or disclosure of protected health information ("PHI").

Notice must occur no later than 60 days after discovery of the breach (*i.e.*, when at least one employee of the entity knows or should have known of the breach). Notice is also required to be provided to media outlets if the information of more than 500 individuals has been compromised. Notification must also be forwarded to HHS.

What is Secured PHI?

On April 27, 2009, HHS issued the HITECH Breach Notification Guidance specifying the technologies and methodologies that render PHI "unusable, unreadable, or indecipherable to unauthorized individuals." That guidance creates a safe harbor so that covered entities and business associates would not be required to provide the breach notifications required by the Act for PHI meeting these standards. PHI is rendered "unusable, unreasonable, or indecipherable to unauthorized individuals" ***only*** if one or more of the following methods are used:

(1) **Encryption.** Electronic PHI is only secured where it has been encrypted. The HIPAA Security Rule specifies the term "encryption" to mean the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. The Rule identifies the various encryption processes which are judged to meet this standard. Further, such confidential process or key that might enable decryption must not have been breached. To avoid a breach of the confidential process or key, decryption tools should be kept on a separate device or at a location separate from the data they are used to encrypt or decrypt.

(2) **Destruction.** Hard copy PHI, such as paper or film media, is only secured where it has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

Determining Whether a Breach of Unsecured Protected Health Information Has Occurred

The Rule states that covered entities and their business associates must analyze the following in determining whether a breach of unsecured PHI has occurred:

(1) **Determine whether the use or disclosure of PHI violates the HIPAA Privacy Rule.**

For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. For example, if information is de-identified in accordance with 45 CFR 164.514(b), it is not PHI and any inadvertent or unauthorized use or disclosure of such information will not be considered a breach under the notification requirements of the Act and the Rule.

(2) **Analyze whether there is a use or disclosure that compromises the security and privacy of PHI**.

HHS clarifies that a use or disclosure that "compromises the security and privacy of PHI" means a use or disclosure that "poses a significant risk of financial, reputational, or other harm to the individual." Thus, in order to determine whether a breach has occurred, covered entities and business associates will need to conduct a risk assessment to determine whether the potential breach presents a significant risk of harm to individuals as a result of an impermissible use or disclosure of PHI. The Rule provides a number of factors which should be taken into account when conducting a risk assessment. A covered entity should consult its legal counsel with respect to the impact of the presence of such factors.

(3) **Assess Whether any Exceptions to the Breach Definition Apply.**

The Rule discusses a number of exceptions to the definition of breach. The following three situations are excluded from the definition of "breach" under the Act:

(i) The unintentional acquisition, access, or use of PHI by any workforce member or person acting under the authority of a covered entity or 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 by the Privacy Rule.

(ii) The inadvertent disclosure of PHI by an individual otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another person at the same covered entity or business associate, or at a 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.

(iii) An unauthorized disclosure where a covered entity or business associate has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

The covered entity or business associate has the burden of proving why a breach notification was not required and must document why the impermissible use or disclosure fell under one of the exceptions. Covered entities should document the risk and other breach assessments accordingly.

Notification Requirements to Individuals and /or Media in the Event of a Breach of Unsecured PHI

The breach notifications required by the Act and the Rule are significant and are triggered by the "discovery" of the breach of unsecured PHI. A breach is treated as "discovered" by a covered entity as of the first day the breach is known, or reasonably should have been known, to the covered entity. Given that knowledge of a breach may be imputed, a covered entity should implement reasonable breach discovery procedures.

Notification to Individuals

A covered entity must send the required notification to each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach, without unreasonable delay and in no case later than 60 calendar days after the date the breach was first discovered by the covered entity. The Act and the Rule specify the content requirements and the methodology required for providing such breach notices.

For covered entities that do not have sufficient contact information for some or all of the affected individuals, the Rule requires that a substitute notice be provided as soon as reasonably possible. If a covered entity has insufficient contact information for 10 or more individuals, then substitute notice must be provided via a posting for a period of 90 days on the home page of its web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. In such instances, the covered entity is also required to have an active toll-free number for 90 days so that an individual can find out whether his or her unsecured PHI may be included in the breach.

Notification to Media

If a covered entity discovers a breach affecting more than 500 residents of a state or jurisdiction, it must provide notice to prominent media outlets serving that state or jurisdiction without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered by the covered entity.

Notification to HHS

If more than 500 individuals are involved in the breach, regardless of whether the breach involved more than 500 residents of a particular State or jurisdiction, then the covered entity must notify HHS concurrently with the individual notifications. For breaches involving fewer than 500 individuals, the covered entity must maintain an internal log or other documentation of such breaches and annually submit such log to HHS. For calendar year 2009, the covered entity is only required to submit the log for breaches occurring on or after September 23, 2009.

Notification by a Business Associate

Following the discovery of a breach of unsecured PHI, a business associate is required to notify the covered entity of the breach so that the covered entity can, in turn, notify the affected individuals. To the extent possible, the business associate should identity each individual whose unsecured PHI has been, or is reasonably believed to have been, breached. Such notice should be given without unreasonable delay and no later than 60 days following discovery of a breach.

Delay Required by Law Enforcement

The Act provides that a breach notification may be delayed if a law enforcement official determines that such notification would impede a criminal investigation or cause damage to national security.

Changes To HIPAA Enforcement

With the enactment of HITECH, HIPAA's enforcement power is much stronger than before:

- Criminal penalties can now be enforced against individuals, including employees of a covered entity. The scope of activities subject to criminal prosecution is broadened to include individuals who obtain or disclose individual PHI "without authorization."

- HITECH clarifies that HHS or state attorneys general can pursue civil penalties in cases where criminal penalties could attach but the Department of Justice declines to pursue the case. Civil monetary penalties are mandatory where a violation due to "willful neglect" has occurred.

- HIPAA penalties will now be based on the level of the violation, with discretion given to HHS on the nature and extent of the harm. Penalties will top out at $50,000 per violation with an annual maximum of $1.5 million for repeat violations of the same provisions. HHS is precluded from imposing civil penalties (except in cases of willful neglect) if violations are corrected within 30 days.

- HITECH expressly authorizes all state attorneys general to enforce HIPAA in federal district court. This provision gives attorneys general the power to enforce the law even if there is no state authorizing statute (but HHS reserves the right to intervene in the action). However, if the state attorney general brings the action, the penalties are the same as the former maximums under the preceding version of HIPAA - $100 per day, $25,000 annual maximum for repeat violations.

Notice: Legal Advice Disclaimer

The purpose of these materials is not to act as legal advice but is intended to provide human resource professionals and their managers with a general overview of some of the more important employment and labor laws affecting their departments. The facts of each instance vary to the point that such a brief overview could not possibly be used in place of the advice of legal counsel.

Also, every situation tends to be factually different depending on the circumstances involved, which requires a specific application of the law.

Additionally, employment and labor laws are in a constant state of change by way of either court decisions or the legislature.

Therefore, whenever such issues arise, the advice of an attorney should be sought.

Scott Warrick, JD, MLHR, CEQC, SPHR

Scott Warrick's Consulting & Employment Law Services

(614) 367-0842 Office ♣ (614) 738-8317 Cell ♣ (614) 367-1044 FAX

www.scottwarrick.com

CEO Magazine's 2008 Human Resources "Superstar"

Nationally Certified Emotional Intelligence Counselor

2008, 2007, 2006 and 2003 SHRM National Diversity Conference Presenter

Scott Trains Managers and Employees ON-SITE in over 40 topics

Scott uses his unique background of **LAW** and **HUMAN RESOURCES** to help organizations avoid legal pitfalls while also helping them improve their employee relations and communication skills.

Scott travels the country presenting his revolutionary **"Emotional Intelligence, Tolerance & Diversity for White Guys … And Other Human Beings: FINALLY A Program For Everyone."** This one of a kind **SKILL-BASED** program creates an atmosphere of open communication so we are better able to resolve all kinds of conflicts in our organizations.

Scott's unique program is the ONLY Diversity/Tolerance Program in the country approved by HRCI-SHRM for STRATEGIC SPHR Credit because unlike most other EI/Diversity/Tolerance Programs, this program goes right to YOUR BOTTOM-LINE.

Scott's clients include the Adena Health Systems, St. Rita's Hospital, Ohio Department of Administrative Services, the Office of Housing and Urban Development, the Bayer Corporation, The Ohio State University, Area Agency on Aging, the Nebraska Army/National Guard, Heinz Frozen Foods, Boeing, EBMC, Honeywell, International Truck & Engine, MTD Products (Cub Cadet, Troy-Bilt & Bolens Lawn Products), etc.

Scott's academic background and awards include:

- Capital University College of Law (Class Valedictorian (1st out of 233))
- Master of Labor and Human Resources and B.A. in Organizational Communication: The Ohio State University
- The Human Resource Association of Central Ohio's Linda Kerns Award for Outstanding Creativity in the Field of Human Resource Management and the Ohio State Human Resource Council's David Prize for Creativity in Human Resource Management

Solving Employee Problems BEFORE They Happen!