



**PREPARED BY**



Michael Smith

600 Congress Avenue  
Suite 1600  
Austin, Texas 78701  
512.499.3650




michael.smith@  
strasburger.com

**EDITORS**

David K. Meyercord  
C. Scott Nichols

**HEALTH INDUSTRY  
GROUP**

Debra W. Biehle  
Thomas W. Burton  
Merritt M. Clements  
Kathryn Midboe Darling  
William Duane Darling  
Richard D. Fladung  
R. Bradley Fletcher  
Brian G. Hamilton  
James M. Kimbell  
David K. Meyercord  
Stuart Miller  
Crawford Moorefield  
Craig H. Myers  
C. Scott Nichols  
Laura Reilly O'Hara  
Jeffrey S. Osgood  
David L. Ovard  
Patrick Owens  
Paul W. Sheldon  
John A. Tang  
Joseph A. Turano  
Melissa W. Shrewsbury  
Carol D. Williamson  
Ivan Wood  
Kevin M. Wood

-  [Printer friendly page](#)
-  [View as Acrobat PDF](#)
-  [Subscribe to HIO RSS](#)

## HHS Issues Security Guidance on Risk Analysis

As discussed in a prior edition of [Health Industry Online](#), the enactment of the American Recovery and Reinvestment Act of 2009<sup>1</sup> (ARRA), and more specifically, Title XIII of the ARRA, known as the Health Information Technology for Economic and Clinical Health Act (HITECH Act) has caused many health care providers and business associates to revisit their existing policies and procedures relating to compliance with HIPAA and its privacy and security regulations.<sup>2</sup>

To assist organizations in complying with HIPAA security standards, the HITECH Act requires the U.S. Department of Health and Human Services (HHS) to issue annual guidance on the "most effective and appropriate technical safeguards" for use in carrying out the provisions of the HIPAA security regulations (Security Rule).<sup>3</sup> Accordingly, HHS will release a series of guidance materials to assist organizations in identifying and implementing administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information (e-PHI), which will be updated annually.

The first annual guidance on the Security Rule, entitled "HIPAA Security Standards: Guidance on Risk Analysis" (Draft Guidance) was recently issued by the HHS Office for Civil Rights (OCR). The Draft Guidance addresses the Security Rule's risk analysis provision, which requires an organization to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of e-PHI held by the covered entity.<sup>4</sup> The Draft Guidance describes risk analysis as the first step in Security Rule compliance, as the outcome of the analysis process is "a critical factor in assessing whether an implementation specification or equivalent measure is reasonable and appropriate."

While the Draft Guidance does not mandate a "one-size-fits-all" method for conducting risk analysis, it does set out the following elements that should be incorporated into any organization's assessment of current security measures and potential risks to e-PHI.

**Scope of the Analysis** – Risk analysis should take into account all e-PHI the organization creates, receives, maintains or transmits, regardless of its form (*i.e.* hard drive, floppy disk, CD) or location (*i.e.* workstation, network).

**Data Collection** – Identify and document where all e-PHI is stored, received, maintained or transmitted.

**Identify and Document Potential Threats and Vulnerabilities** – Identify threats to e-PHI security that may be unique to the organization's environment and document vulnerabilities or weaknesses in current security procedures or design.

**Assess Current Security Measures** – Assess and

document whether required security measures to safeguard e-PHI are in place and if current measures are properly utilized.

**Determine Likelihood of Threat Occurrence** – Determine the probability of potential threats to e-PHI security and identify those that may be reasonably anticipated.

**Determine Potential Impact of Threat Occurrence** – Determine the potential impact of exploitation of certain weaknesses or flaws in e-PHI security.

**Determine the Level of Risk** – Analyze the likelihood and the potential impact of identified security threats and vulnerabilities and identify actions that may mitigate such risks.

**Finalize Documentation** – Document the risk analysis; no specific format is required.

**Periodic Review and Updates to the Risk Assessment** – Conduct continuous risk analysis to identify when security updates are needed and prepare for changes in the organization's operations or structure.

Risk analysis should be an ongoing process and methodology will vary based on the size, complexity, and capabilities of each organization. While the Draft Guidance is not a "one-size-fits-all" blueprint for all covered entities or business associates, it does provide insight into the expectations of HHS and offers assistance to organizations working to comply with the Security Rule.

A link to the Draft Guidance is available on the OCR website:

[www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidanceintro.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidanceintro.html).

**ALERT** – On July 8, 2010, the OCR released its Notice of Proposed Rulemaking for implementation of new and amended HIPAA rules in light of the HITECH Act. The proposed rules, once adopted, will modify the Privacy, Security, and Enforcement Rules originally issued under HIPAA. According to comments by Secretary Sebelius, the proposed rules will strengthen and expand enforcement of HIPAA by:

- expanding individuals' rights to access their information and to restrict certain types of disclosures of protected health information to health plans;
- requiring business associates of HIPAA-covered entities to be under most of the same rules as covered entities;
- setting new limitations on the use and disclosure of protected health information for marketing and fundraising; and
- prohibiting the sale of protected health information without patient authorization.

Comments to the proposed rules may be submitted for 60 days following publication in the Federal Register, which is expected on July 14, 2010. A copy of the proposed rule can be viewed at:

[www.ofr.gov/OFRUpload/OFRData/2010-16718\\_PI.pdf](http://www.ofr.gov/OFRUpload/OFRData/2010-16718_PI.pdf).

---

<sup>1</sup> American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 (2009). The ARRA was enacted February 17, 2009.

<sup>2</sup> See 45 C.F.R. Pts. 160 and 164.

<sup>3</sup> See 45 C.F.R. §§ 164.302 – 318.

<sup>4</sup> 45 C.F.R. § 164.308(a)(1)(ii)(A).

**PUBLICATIONS:**

- To view past issues of Health Industry Online, please visit [Health Industry Online](#)
- To subscribe to other Strasburger publications, please visit [Strasburger Publications](#)

**DISCLAIMER:** Articles contained within this newsletter provide information on general legal issues and are not intended to provide advice on any specific legal matter or factual situation. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional counsel.

**ADVERTISEMENT NOTICE:** This e-mail may constitute a commercial electronic mail message subject to the CAN-SPAM Act of 2003. If you do not wish to receive further commercial electronic mail messages from the sender, please send an e-mail to [Strasburger@Strasburger.com](mailto:Strasburger@Strasburger.com) and request that your e-mail address be removed from future mailings. To update your address, please send an email to [Strasburger@Strasburger.com](mailto:Strasburger@Strasburger.com) including the updated information. Strasburger & Price, LLP, 901 Main Street, Suite 4400, Dallas, TX 75202.

