OBER | KALER
Attorneys at Law

www.ober.com

# HIPAA and Health Care Information Technology

## Government Issues Draft of First Annual Security Guidance

**July 2, 2010**

James B. Wieland
410.347.7397
jbwieland@ober.com

The HIPAA Security Rule, which is basically a series of technologically neutral touch points for developing HIPAA compliant processes and procedures for safeguarding protected health information in electronic form ("e-PHI"), has been in effect for nearly ten years now, but has generally received less attention than has the HIPAA Privacy Rule. Many smaller covered entities, lacking an in-house technology resource and using systems purchased or licensed from third parties, have relied upon vendors or licensors for Security Rule compliance. However, as the health care system moves inexorably towards electronic health records and as more and more protected health information is stored and moved in electronic form, all covered entities are turning their attention to the security of their information systems.

The Office of Civil Rights in the Department of Health and Human Services, an important component of the government's HIPAA education and enforcement efforts, has published a draft of its first annual guidance on the provisions of the HIPAA Security Rule: HIPAA Security Standards: Guidance on Risk Analysis (the "Draft Guidance"). The publication of "official" annual guidance is required by the HITECH Act and the risk assessment is an appropriate starting place, since the risk assessment is the foundation for all of the ePHI security measures and procedures that covered entities actually adopt. It is not enough to be secure, at least under the HIPAA

Security Rule; the HIPAA Security Rule requires documentation of the decision making process that led each covered entity to select the means of achieving security for e-PHI at rest in or transmitted by the covered entity. The risk assessment is described in the Security Rule as "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."

The Draft Guidance points out that the Security Rule does not require a specific, "one-size-fits-all" form or format for the risk analysis: ". . . methods will vary depending on the size, complexity, and capabilities of the organization." As the Draft Guidance also notes, the risk assessment is a required element of compliance, in contrast to the many other elements that are addressable by alternative means reasonably selected by the covered entity: ". . . the Rule indentifies the risk analysis as the foundational element in the process of achieving compliance and it establishes several objectives that any methodology adopted must achieve." It is the foundation for the measures chosen because ". . . the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate."

The Draft Guidance suggests three basic areas that covered entities should consider: (i) identification of e-PHI that the organization creates, receives, maintains, or transmits; (ii) identification of external sources of e-PHI, including vendors and consultants; and (iii) the human, natural, and environmental threats to information systems that contain e-PHI.

Information gained from the risk assessment, the Draft Guidance suggests, can be used for a number of purposes in attaining compliance with the other requirements of the Security Rule, including: (i) design of appropriate personnel processes; (ii) identification of what data to back-up and how to do so; (iii) the decision as to whether or not to use encryption[1]; (iv) addressing which information must be authenticated in particular situations to protect data integrity; and (iv) determining the appropriate manner for protecting electronic transmissions of protected health information.

[1] Encryption is an "addressable" element of the Security Rule. It is not required and alternative measures may satisfy the Security Rule. However, while encryption typically requires changes to a covered entity's internal processes, the cost has gone down significantly in the years since the issuance of the Security Rule. At least two states appear to require encryption as to personal information of individuals in a third party's hands, under laws generally related to consumer protection but of potential application to certain protected health information. Finally, in general, both under most state's laws requiring notification of individuals if an individual's personal information in a third party's hands is compromised and under the HITECH Act Breach notification requirements, notification is *not* required if the electronic personal information/protected health information, was encrypted. The HITECH Act specifies the specific standards that must be used for encryption; most state laws are silent of the specific standards. In the author's view, this significantly alters the cost/benefit analysis as to encryption in favor of encryption.

The Draft Guidance provides definitions of certain important terms that are not defined in the Security Rule: Vulnerability; Threat; and Risk. The bulk of the Draft Guidance is devoted to consideration of the elements of performing the risk analysis, including:

- The scope of the recommended analysis, which must take into account all of the organizations e-PHI;

- Data collection, which must identify the locations at which e-PHI is stored, maintained or transmitted;

- The potential risks and vulnerabilities that must be identified, which include all reasonably anticipated threats;

- An assessment of current security measures, which must be identified and documented. This element is particularly important, even for organizations that performed a risk analysis in 2003 when the Security Rule became effective, since as was pointed out in the Security Rule and as is restated in this portion of the Draft Guidance, risks change over time. The Draft Guidance, as to this element, specifically states that the organization must determine whether existing measures are configured and used properly.

- The likelihood of a threat occurrence, which will determine which threats require corresponding measures because they are "reasonably anticipated";

- The potential impact of threat occurrences on the confidentiality, integrity, and availability of e-PHI, under qualitative and/or quantitative methods; and

- A determination of the level of risk for each threat and vulnerability that is identified in the risk analysis, which will determine the list of corrective actions that will be developed for each risk.

The Draft Guidance concludes by repeating the need to document all elements of the risk assessment and the need for periodic review and updates. The Draft Guidance gives the following example: ". . . if the covered entity has experienced a security incident, has a change in ownership, turnover in key personnel, is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected." Audits of Security Rule compliance appear to be becoming more common, especially in the event of a breach, as defined in the HITECH Act, involving 500 or more individuals, which must be reported promptly to the Secretary of the Department of Health and Human Services. Updates are

likely to be an important audit point, in the event that the organization is subject to an audit of its compliance with the Security Rule.

The Draft Guidance mentions NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Revision 1 (October 2008). The subtitle for the document is "An Introductory Resource Guide for Implementing the Health Insurance Portability Act (HIPAA) Security Rule." This is a useful document for those who wish to get more deeply into the process. NIST, the Department of Commerce National Institute of Standards and Technology, is generally authoritative as to the details underlying the HIPAA Security Rule. The Draft Guidance provides a link to NIST publication 800-30 on the NIST website. A complete list of all the NIST publications relating to information security can be found on the NIST website itself, at http://csrc.nist.gov/publications/PubsSPs.html. Those who choose to access this NIST document other than through the OCR link should be careful to get Revision 2 to Special Publication 800-30, dated October 2008, since the earlier version is still available from NIST.

A complete copy of the Draft Guidance can be found at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidanceintro.html.

---

**About Ober|Kaler**

Ober|Kaler is a national law firm that provides integrated regulatory, transaction and litigation services to financial, health care, construction and other business organizations. The firm has more than 120 attorneys in offices in Baltimore, MD, Washington, DC and Falls Church, VA. For more information, visit www.ober.com.

---