2010 Volume 2

www.ober.com

IN THIS ISSUE

HIPAA: The New Enforcement Culture

By: James B. Wieland

Ober|Kaler's Health Law attorneys are regular contributors to Medical Laboratory Observer's "Liability and the Lab" column at mlo-online.com. This article appears in the November 2010 edition.

The culture of HIPAA compliance is about to change, driven by significant changes in the law. The OIG has been encouraging a "culture of compliance" with the antikickback laws for a number of years, which has resulted in a general awareness in clinical laboratories. Most in the health care industry, for example, know that giving a physician something of value to reward referrals is not acceptable. Few are likely to know what the foundation for compliance with the HIPAA Security Rule is, but that is changing as well.

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 (ePHI) has been in effect for nearly 10 years now, but has generally received less attention than has the HIPAA Privacy Rule. The federal HIPAA enforcers have published a draft of their first annual guidance on the provisions of the HIPAA Security Rule: HIPAA Security Standards: Guidance on Risk Analysis (the Draft Guidance). Under the HIPAA Security Rule, it is not enough to be secure; documentation of the decision-making process that led each clinical laboratory or other HIPAA-covered entity to select the means of achieving security for ePHI at rest in or transmitted by the covered entity is required. 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The Draft Guidance points out that the Security Rule does not require a specific, "one-size-fits-all" form or format for the risk analysis: "[M]ethods will vary depending on the size, complexity, and capabilities of the organization." 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: "[T]he 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." A complete copy of the Draft Guidance is available at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidanceintro.html.

To date, violations of HIPAA have generally been met by the HIPAA enforcers with an educational, rather than a punitive, response; however, spurred on by Congress, a more sanction-oriented approach is being implemented. Add to this the fact that HIPAA now requires that a breach of unsecured protected health information must be reported to the government, and the groundwork for a sanction-driven culture change is set.

Under HIPAA, as amended by the Health Information for Economic and Clinical Health (HITECH) Act, the government is required to investigate all reported situations that indicate willful neglect in connection with a violation. If the investigation confirms that a violation was due to *willful neglect*, the Secretary is required to impose a Civil Monetary Penalty (CMP). The Secretary maintains the ability to respond to violations that do not involve willful neglect with educational efforts. The HITECH Act established a new tiered system that reflects increasing levels of culpability and corresponding penalty amounts that significantly increase the minimum penalty amount for each violation.

The penalty for a violation due to willful neglect is $10,000 for each such violation, subject to a cap for all such violations of an identical requirement during a calendar year of $250,000 — if the violation was corrected within 30 days. If the violation was not corrected within 30 days, the penalty is $50,000 for each such violation, subject to a cap for all such violations of an identical requirement during a calendar year of $1,500,000. Based on past practice, the first documents an investigator is likely to ask for are the risk assessment, and the resulting policies and procedures for the physical, administrative, and electronic security of ePHI.

Many smaller covered entities that lack an in-house technology resource and use systems purchased or licensed from third parties have relied upon vendors or licensors for the security of their electronic records. 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 should be paying attention to the security of their information systems, because the culture of HIPAA compliance is changing.