Reinhart

OIG Conducting HIPAA Security Rule Compliance Audits: HIPAA Security Should Be a Priority for All Covered Health Care Entities

POSTED:

Jul 1, 2007

RELATED PRACTICES:

Health Care

https://www.reinhartlaw.com/practices/health-care

The Department of Health and Human Services' Office of Inspector General ("OIG") is currently in the process of conducting audits of covered health care entities for compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule.[1] It appears as though these audits signal the beginning of an increase in the OIG's focus on Security Rule investigation and enforcement efforts. An overview of the OIG's audit initiative and the reasons for its increased focus on Security Rule compliance and recommendations for Security Rule compliance are outlined below.

1. The OIG Security Rule Audit Initiative

The OIG recently began Security Rule compliance audits on HIPAA-covered health care entities. The first of these audits took place in March of this year and focused on an Atlanta hospital's administrative, physical and technical safeguards for electronic-protected health information ("e-PHI")-the core requirements under the Security Rule. Unlike audits involving the HIPAA Privacy Rule, which are primarily complaint driven, current Security Rule compliance audits that have been confirmed have not been the result of complaints to the OIG.

An indication of the OIG's new investigation and enforcement efforts was given in the 2007 OIG Work Plan-where the OIG noted that it would:

> review the experience with the [HIPAA] administrative simplification privacy and security implementation in Medicare and Medicaid to identify key issues that may be relevant to the Department [of Health and Human Services'] health information technology (IT) initiative. The Department's health IT initiative has a primary objective of fostering the use of electronic medical records throughout the health industry to promote economy and efficiency in the delivery of health services and to enhance patient safety.[2]

The Centers for Medicare and Medicaid Services ("CMS"), which oversees Security Rule enforcement, has not proactively investigated covered entities for Security

Rule compliance since the Security Rule's 2005 effective date. Rather, CMS largely depended on voluntary compliance to ensure HIPAA's effectiveness. Concerns with voluntary compliance efforts have likely caused the OIG to increase its investigation/enforcement efforts through its Security Rule compliance audits.

2. The OIG Is Concerned About Voluntary Security Rule Compliance and Security Breaches Involving e-PHI

The OIG's audit initiative is most likely the result of concerns with voluntary Security Rule compliance efforts. In fact, in its 2007 Work Plan, the OIG stated that "[t]he wider use of electronic medical records and personal health records raises concerns over privacy and security of patient data.[3]" This concern may be driven, in part, by the high profile of many security breach incidents involving e-PHI that have occurred over the last several months. Many of these security breaches involved lost or stolen laptop computers with inadequate security and occurred both in and out of the health care industry, including several at the Department of Veterans Affairs.

Note that CMS also appears to be concerned by recent security breaches and Security Rule compliance efforts. In fact, on December 28, 2006, CMS published guidance entitled, "HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information,"[4] which was intended to reiterate ways that covered entities" may protect e-PHI when it is accessed or used outside of the organization's physical purview."[5]

3. Complying with the Security Rule

Given the OIG's Security Rule audit initiative and its concern with voluntary compliance efforts, HIPAA security should be at an elevated priority level for covered entities.

As stated above, the Security Rule requires administrative, physical and technical safeguards for e-PHI. Each of these safeguard categories includes specific standards. For each standard, the Security Rule provides a number of "implementation specifications." In all, there are over 40 implementation specifications and each is either "required" or "addressable."[6] Covered entities must meet all of the required implementation specifications and should assess in writing the reasonableness and applicability of those that are addressable.

Because of the complex and technical nature of the Security Rule and its implementation specifications, it is important for covered entities (or their information security officers) to become familiar with its requirements. Once familiar with the Security Rule, covered entities should consider taking the following steps in furtherance of Security Rule compliance:

- Perform a comprehensive risk assessment. The Security Rule requires that a risk assessment be undertaken by covered entities to assess thoroughly the potential risks and vulnerabilities to the confidentiality, integrity and availability of e PHI that is maintained. A new risk assessment should be conducted annually or when there is any significant environmental changes. As part of the risk assessment, covered entities should keep track of where they are storing e PHI-both within the internal electronic environment and externally through remote devices and storage media.
- Once the risk assessment is complete, follow through to make sure that the problems identified are corrected. Note that risk management does not mean fixing every threat identified. Risks should be prioritized and action should be taken accordingly.
- Conduct regular audits. The Security Rule requires covered entities to conduct regular audits by logging certain events related to e-PHI and reviewing those logs regularly. Logging such events (e.g., recording each time someone accesses an individuals e-PHI) is generally done automatically through software.
- Make sure there are appropriate policies and procedures in place. The Security Rule requires that there be a detailed process by which vulnerabilities are assessed and appropriate safeguards are implemented. The policies and procedures should be accurate, complete, communicated to employees and enforced.

When developing Security Rule compliance strategies, covered entities may want to use the National Institute of Standards and Technology's ("NIST") SP 800 66, *An Introduction Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. The NIST guide is intended for government agencies and contains more detailed information than the Security Rule. For more information or individualized consultation regarding Security Rule compliance, please do not hesitate to contact a member of the Health Care Department at *Reinhart Boerner Van Deuren s.c.*

[1] 45 C.F.R. Parts 160 and 164; 68 Fed. Reg. 8334 (Feb. 20, 2003) (available at *http://www.cms.hhs.gov/0SecurityStandard/Downloads/securityfinalrule.pdf*).
[2] HHS OIG FY 2007 Work Plan 45 (available at *http://oig.hhs.gov/publications/docs/workplan/2007/ Work%20Plan%202007.pdf*).
[3] Id.
[4] Available at *http://www.cs.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal.pdf*
[5] Id. at 1.
[6] The safeguard categories, standards and implementation specifications are set forth in a matrix at the end of the Security Rule (available at *http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf*).