HIPAA Phase 2 Audits Begin: What Are The Risks?

PUBLISHED ON

April 7, 2016

On March 21st, OCR*1* commenced Phase 2 of its HIPAA*2* Audit Program. OCR will audit health plans, hospitals, physician groups and other healthcare entities for compliance with HIPAA's Privacy, Security and Breach Notification Rules. A primary focus of OCR's audits will be assessing the security of "protected health information" ("PHI"), and the prevention of PHI breaches.

OCR has begun sending its pre-audit questionnaire to a broad range of healthcare entities (large and small). Although randomly selected, respondents will be asked to provide information that reveals the size of their organizations in terms of total revenue and operations (e.g., number of hospital beds, number of clinicians, number of health plan members/claims, etc.). From this information, OCR will create a target list of entities to be selected for desk audits.

Desk audits will be completed by December 2016 and will focus largely on the deficiencies uncovered during the Phase 1 audits, including: failure to conduct periodic security risk assessments; missing, outdated or deficient privacy/security policies and controls; and inadequate HIPAA training. In addition, unlike the Phase 1 audits, the Phase 2 audits will include covered entities and business associates. Respondents will be asked to identify and list all of their business associates.

Based upon the results of the desk audits, OCR will select a small number of auditees for on-site audits. Before final selection, auditees will be given the opportunity to respond to OCR's desk audit findings and explain why an on-site audit may not be necessary, and what corrective actions will be taken. While on-site audits will be few in number, OCR will employ "enhanced" protocols*3* to target potential HIPAA violations and those auditees that may require a site visit.

If an on-site audit is conducted, OCR will talk with management, privacy/security officer(s), IT personnel, employees and others in soliciting reports or complaints of possible HIPAA violations. Although OCR has indicated that HIPAA audits are not intended to be punitive, and will be used primarily to recommend technical improvements or other corrective actions, OCR intends to impose monetary penalties for serious violations.

So what are the potential risks or concerns? During the Phase 1 audits, Security Rule violations topped the list of OCR findings. Thus, it is anticipated that Security Rule compliance will be a primary focus of OCR's Phase 2 audits. This also is consistent with the recent pattern of OCR enforcement actions in which HIPAA fines are on the rise at $28MM and counting.

OCR's most serious enforcement actions and penalties have resulted from PHI security mishaps and breaches, including OCR's recent $1.5MM settlement with North Memorial Health Care of Minnesota. This healthcare system agreed to settle charges by OCR that it failed to properly secure the PHI of nearly 9,500 individuals contained on a laptop that was stolen from a business associate's vehicle.

While OCR's Phase 1 audits were designed to "encourage" HIPAA compliance, the Phase 2 audits will be "real" audits with financial penalties and consequences. In other words, this time it's serious. Healthcare entities should not wait to begin preparing for a HIPAA audit. Receipt of a HIPAA audit request is only a matter of time. After Phase 2, OCR intends to establish its HIPAA Audit Program as a permanent compliance program. With penalties up to $50,000 per violation, HIPAA compliance is a lucrative area for government audits and investigations, and enforcement actions will continue in earnest.[4]

Therefore, healthcare entities should begin now in assessing their HIPAA compliance. This includes: updating privacy/security policies and procedures; implementing training programs; assigning privacy/security officer responsibilities; and creating a HIPAA audit team, with IT and other key personnel, to evaluate and strengthen PHI controls.[5] In addition, any prior mishandling of PHI breaches/notifications should be resolved now before OCR's HIPAA auditors arrive.

If a HIPAA audit request is received, the organization will have only 10 days to respond. Start by focusing immediate attention on PHI security and the proper handling of PHI breaches. Since these are the most serious potential violations, compliance in this area should be a top priority, and the best place to begin.

If you have questions concerning the HIPAA Phase 2 Audit Program, please call Chris Churchill, Partner and Chair of Barley Snyder's Health Law Group, at 717-399-1571, or contact him at cchurchill@barley.com.

[1] Office of Civil Rights of the U. S. Department of Health and Human Services.
[2] Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH"), as part of the American Recovery and Reinvestment Act of 2009.
[3] OCR's current HIPAA audit protocols exceed 400 pages and are available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase1/index.html.
[4] Recently, another government agency, the Federal Trade Commission-with authority over security breaches affecting consumers' personal health records, has taken steps to expand its own enforcement actions and the ability to impose civil penalties for data security breaches.
[5] To help healthcare entities improve PHI security, OCR has published a crosswalk, developed with the National Institute of Standards and Technology ("NIST") and others, that identifies "mappings" between the NIST Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework") and the HIPAA Security Rule. This crosswalk is available at http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/.

:

Christopher J. Churchill

Partner

Tel: (717) 399-1571

Email: cchurchill@barley.com