DATA SECURITY AND PRIVACY ALERT

JUNE 24, 2015

SHOOK
HARDY & BACON

HIPAA AUDIT PROGRAM: IS PHASE 2 ALMOST HERE?

by Dan Rohner

The Office of Civil Rights (OCR) within the U.S. Department of Health and Human Services (HSS) is distributing preliminary HIPAA compliance surveys and preparing for a second round of HIPAA compliance audits. All HIPAA-covered entities and their business associates should take steps now to be prepared to respond.

HIPAA Audits – Phase 1

Under the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH), OCR is required to conduct HIPAA compliance audits of covered entities and their business associates. The OCR HIPAA Audit program was designed to review and analyze the processes, controls and policies of selected covered entities pursuant to the HITECH Act audit mandate.

As part of a pilot phase for the audit program ("Phase 1"), OCR identified a pool of 115 covered entities for audits that broadly represented the wide range of healthcare providers, health plans and healthcare clearinghouses operating today. OCR also established a comprehensive audit protocol identifying the requirements to be assessed. The protocol was organized around modules, representing the following separate elements:

- PRIVACY – The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for protected health information (PHI), (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.
- SECURITY – The protocol covers Security Rule requirements for administrative, physical and technical safeguards.
- BREACH NOTIFICATION – The protocol covers requirements for the Breach Notification Rule.

See U.S. Department of Health & Human Services, *HIPAA Privacy & Security Audit Program*.

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Data Security and Privacy capabilities, please visit shb.com or contact:

Al Saikali
dd 305.960.6923
asaikali@shb.com

Dan Rohner
dd 303.285.5302
drohner@shb.com

The Phase 1 audits were completed in 2011 and 2012. Since then, OCR has reviewed the data and conducted surveys of the audit participants to evaluate the pilot audit program's effectiveness, analyze the program's strengths and weaknesses, and provide recommendations for how OCR conducts future audits. See *HIPAA Privacy and Security Audit Program*. By all accounts, the results of the Phase 1 audits revealed a number of areas where a large percentage of covered entities are not in compliance. According to Leon Rodriguez, OCR's former director, the Phase 1 audits consistently revealed a lack of thorough risk analysis and failure to comply with the HIPAA breach notification rule. *See* Comments by Leon Rodriguez, 2013 HIMSS Privacy and Security Forum.

HIPAA Audits - Phase 2

In February 2014, OCR filed an information collection request in the *Federal Register* indicating its intent to send a survey to up to 800 covered entities and 400 business associates (entities that provide certain services to a HIPAA-covered entity). *See* 79 FR 10158, 10158-59. OCR explained that the purpose of the surveys was to enable OCR to determine suitability (*i.e.*, size, complexity and fitness) of each survey respondent for a Phase 2 audit. *See* 79 FR at 10159. The information to be collected included, among other things, recent data about the number of patient visits or insured lives, use of electronic information, revenue, and business locations. *Id.*

OCR had expected that the survey would be sent over the summer and that the Phase 2 audit program would begin during fall 2014. Shortly after the February 2014 announcement, however, OCR announced that it was delaying the surveys and the audits to create an online portal through which covered entities and associates could submit audit information. As of March 2015, OCR Director Jocelyn Samuels, speaking at the 23rd National HIPAA Summit, said that the second phase of the program was "still under development," adding that the portal was "still in the process of being set up."

Recent reports, however, now suggest that OCR is finally prepared to move forward with the Phase 2 audits. In May, a randomly selected pool of covered entities received the preliminary surveys referenced in last year's information collection request. While OCR has yet to announce an exact date when the next round of HIPAA audits will occur, based on the

timeline proposed last year, there is a strong likelihood OCR could begin performing Phase 2 audits as early as fall 2015.

How Are Phase 2 Audits Different from Phase 1?

Unlike the pilot audits during 2011 and 2012, which focused on covered entities, OCR will conduct its Phase 2 audits on covered entities and their business associates. Based on the responses to the surveys, OCR will select approximately 350 covered entities to receive data requests for the Phase 2 audits. Among other things, the data requests will seek the names and contact information for all HIPAA business associates. OCR has indicated that it intends to audit approximately 150 of the 350 selected covered entities and 50 of the selected business associates for compliance with HIPAA's Security Standards.

The Phase 2 audits will also have a more narrow focus than those in Phase 1. Phase 2 will focus on areas of noncompliance revealed by Phase 1, and the greater risk to the security of PHI confirmed by Phase 1's findings and observations. The Phase 2 audits of business associates will focus on risk analysis, risk management and the reporting of HIPAA breaches to covered entities.

Ultimately, the Phase 2 audits are intended to better identify best practices and uncover risks and vulnerabilities that OCR may not have already identified through its enforcement activities. OCR has also stated that it intends to use the Phase 2 audit findings to identify technical assistance that it should develop for covered entities and business associates. That said, participants in these audits should also be aware that if the audit reveals a serious compliance concern, OCR is free to initiate a formal compliance review, which could lead to civil monetary penalties.

What Can You Do Now to Prepare?

Covered entities and business associates should take the following steps now to ensure that they are prepared for a potential Phase 2 audit:

- Reassess whether HIPAA/HITECH are applicable to you (are you a covered entity or, more likely, a business associate);
- If audited, covered entities and business associates will be responsible for showing compliance with aspects of the protocols found to be deficient in many Phase 1 audits, and particularly risk analysis,

risk management and security. Given this focus, it might be a good time to obtain an assessment to identify any security vulnerabilities and prepare a list of action items with proposed completion deadlines. We recommend that the assessment be conducted at the direction of outside counsel so that results may be protected by the attorney-client privilege;

- If you have already completed a security vulnerability risk assessment, confirm (again at the direction of outside counsel) that all previously identified action items have been completed or are on a reasonable timeline for completion and document all ongoing risk management activities;
- For covered entities, sort through all of your vendors and create a list of all HIPAA business associates with their contact information and a description of the services that they provide;
- Review with counsel whether you need to update your policies and procedures, your business associate agreements or your notices of privacy practices;
- Review with counsel whether you need facility security plans, a disaster recovery plan, emergency access procedures, or any other HIPAA security policies given the structure of your organization;
- Confirm that you have a breach notification policy in place that complies with the content and deadline requirements under the Breach Notification Standards;
- Confirm that you are training your employees and contractors to comply with all HIPAA Standards that are necessary or appropriate given their job duties; and
- Encrypt, encrypt, encrypt. All systems and software that transmit electronic PHI should employ encryption technology. If they do not, you must fully document the risk analysis supporting your decision not to encrypt PHI.