WINSTEAD

How Recent Cybersecurity Government Publications Impact HIPAA Security Compliance and the New Audit Initiative

04.04.16

Cybersecurity Impacts on HIPAA Security Compliance and the New Audit Initiative

New Audit Initiative Items to Watch

While The HHS Office for Civil Rights recently announced its intent to perform a second round of HIPAA Privacy, Security and Breach audits via an email initiated process with submissions on its secure website, this is only the beginning of the story. In the announcement they discussed that there will be 10 business days to respond to the initial request that will come via email. The actual letter initiating the review states, "Please respond within fourteen (14) days as instructed below to either confirm your identity and email address or …" and in many cases 10 business days will be about the same as 14 days, but be aware there are two different deadlines in their materials.

If you do not respond to their initial email, the letter states that the OCR will continue to use that email to contact you on the investigation, which raises a number of concerns. *Covered entities need to be checking their email filters to catch emails sent and caught by the filters or sent to former employees or email addresses that may not be currently monitored by an employee (e.g., an email for an employee out on a leave or vacation) to ensure they capture any email that was sent to initiate one of these reviews. Since the OCR will continue to use an email until they are corrected, a covered entity that does not check for emails that might be lost in their system will be doing so at their own peril. Failure to respond to the initial request will not relieve one from the audit or compliance review.*

These are audits of covered entities and business associates. So business associates of health plans and healthcare providers need to be checking their email systems for these audit initiating emails as well. The audits will not be on entities with an open complain investigation or who are already undergoing a compliance review.

The initial audit will include a pre-audit screening questionnaire asking for identification of all of the entity's business associates with their contact information. Health plans and other covered entities may want to prepare an inventory of all of their business associates with contact information for each and business associates should identify all of their subcontractors with contact information.

If after the initial email letter, you are selected for the compliance review/audit, you will be asked to submit additional information via the OCR secure portal within 10 business days of the request and you will be introduced to the OCR audit team and receive an explanation of the audit process. You must be able to submit all documentation digitally. You will receive a draft audit report and have 10 business days to review it and provide written comments. If it is an onsite audit, you can expect that they will be spending 3 to 5 days onsite with you and then will get a draft report with similar times to respond.

The information on the OCR website includes a statement that the Freedom of Information Act ("FOIA") may require the OCR to release audit notification letters and other information about the audits upon request by the public. *If you receive one of the audit letters, it is important to review the FOIA protections you may be able to claim to keep information confidential after you submit it to the OCR. The FOIA can be used to obtain information submitted to some agencies and this may raise some business concerns.*

Importance of Timely Business Associate Agreements

A recent OCR resolution agreement dealt with a covered entity that provided access to PHI to a business associate on March 21, 2011, but did not have a written business associate agreement with that business associate until October 14, 2011, and for its failure to conduct "an accurate and thorough risk assessment of all of its information technology equipment. The resolution agreement required the covered entity to pay $1,550,000 and to implement a corrective action plan which was longer than the resolution agreement. *This reminds us of the importance of getting the business associate agreements done before any PHI is transferred.*

Cybersecurity Developments

The OCR's new audit initiative follows the FBI's recent report on the Internet Crime Complaint Center for 2014 which provides interesting statistics on various scams reported to the FBI, including the government impersonation email scam, business e-mail compromise as well as a variety of scams and other fraudulent activities that it pays to be aware of and consider in keeping an entity's system secure. It may be helpful to consider some of the various schemes when working on educating your personnel on security and protection of the entity and themselves.

While the HIPAA Security regulations have not had significant changes in recent years, the cyber world is continuing to evolve. Since the HIPAA Security regulations permit the entity to implement them as appropriate for their business size, covered entities need to pay attention to the changes that are applying in the industry for the covered entity (including the health plan). In response to recent cyberattacks, the OCR issued its Cyber Awareness Monthly Update which reminds us that cyber threats and attacks are a constant concern because they can cause serious disruptions to operations. It focused on Nation-State Attacks, Ransomware Attacks, Smartphone Attacks and steps that a business can take to protect itself. It also provided links to resources at the FBI to protect against Nation-State attacks and to report internet fraud and the United States Computer Emergency Readiness Team for Ransomware remediation. It contained a list of steps one can take to improve security practices. Device control is very important.

The OCR also issued what it called "A Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework" which provides in a chart format a way for covered entities to look at how compliance with the HIPAA Security Rule can be accomplished under the NIST Cybersecurity standards. *For organizations that have not aligned their HIPAA Security requirements to the NIST Cybersecurity standards, it provides a way to more quickly find your way into the NIST standards that address the HIPAA Security requirements.*