POLICY AND LEGISLATION

Gerry Blass and Susan A. Miller, JD

OCR HIPAA Audits

We Now Know the Protocols

WE SHOULD ALL KNOW BY NOW that the Office for Civil Rights (OCR) has been mandated to audit all HIPAA Covered Entities (CEs) and Business Associates (BAs), and we now know the main ingredients of the audits—the protocols, which are subject to change over time based on audit results. All CEs and BAs should begin a process now to prepare for an OCR audit based on the most current protocols. Why? Because once the OCR notifies you that your organization will be audited, you only have a couple of weeks to prepare.

BACKGROUND

Congress had long grumbled that HIPAA enforcement had no teeth, so within the HITECH Act they mandated that the OCR develop an audit program for all CEs, and BAs of all sizes.

OCR began this program in 2011 with 20 audits, and found that some covered entities had done very little to fulfill the HIPAA privacy, security, and breach-notification requirements. No surprise perhaps!

In 2012 the OCR did 95 more audits and found the same thing, even though the healthcare industry had seen the results of the 2011 audits. Perhaps the missing ingredients surrounding the OCR audits were the audits themselves. How were they being conducted?

GOOD NEWS—PUBLISHED PROTOCOLS

The good news is that in the summer of 2012 the OCR published the audit protocols that the OCR, through KPMG, are using to audit the healthcare industry. The protocols were updated in September 2012. There are a total of 169 protocols—78 for HIPAA security, 81 for HIPAA privacy, and 10 for HIPAA breach. You can find the protocols here.

Susan McAndrew, JD, leader of all things HIPAA-HITECH at the Office for Civil Rights has been speaking at conferences about both the audits and the Omnibus rules since 2009, saying that HIPAA CEs and BAs should have a robust HIPAA Privacy and Security compliance program, including:

- Employee training;
- vigilant implementation of policies and procedures;
- a prompt action plan to respond to incidents and breaches; and
- regular internal audits.

You might remember that these bullets are four of the seven parts that the Department of Health & Human Services (HHS), Office of Inspector General (OIG) had recommended for a healthcare compliance program beginning in 1999.

So why do we think all of this is good news? Because now all CEs and BAs are in a position to know how to prepare for an OCR audit, and have another motivating factor to overcome organizational challenges that they may be dealing with, such as a limited budget or lack of an organizational mandate.

The combination of the OCR audits, the potential large financial penalties and lawsuits and bad press for a breach of protected health information along with CE attestation for Meaningful Use measures, including information security risk analysis, we believe that the healthcare industry is finally sensing a higher financial risk for non-compliance vs. the cost to comply.

For example, a recent industry survey found that the cost is an average of $200 per individual if you have a breach. This alone is $100,000 if you have a violation of no more than 500 individuals. Add to this the millions in fines that OCR is now handing out, plus the cost of mitigation. So, the loss of a laptop may cost many large CEs $2 million, even if they self-report.

THE OCR AUDIT LETTER

The first thing that arrives when you are audited is a letter from OCR and its contractor, KPMG, which includes a two-page list of requested documentation. The obvious requests are for policies and procedures. In addition there are requests for documentation that shows evidence of operational compliance with policies and procedures, such as "HITECH breach notification process, entity-level risk assessment documentation and capabilities." Some documentation in the protocol list may need to be created from scratch based on actual processes. So it will take time to get it all together. You can obtain a copy of the two-page document request free for download here.

THE COMBINATION OF THE OCR AUDITS, the potential large financial penalties and lawsuits and bad press for a breach of protected health information along with CE attestation for Meaningful Use measures, including information security risk analysis, we believe that the healthcare industry is finally sensing a higher financial risk for non-compliance vs. the cost to comply.

INTERESTING POINTS

Here are some interesting points regarding the OCR audits. First, the mandate for the audits is within a law only, the HITECH Act. Second, the audits are not part of the HIPAA general administrative requirements that outline HIPAA enforcement, preemption of state law, compliance and enforcement, imposition of civil money penalties, and procedures for hearing.

However, there is an interconnection between the OCR audits and HIPAA enforcement in that if major HIPAA compliance gaps are identified during an audit OCR will do a further investigation as outlined in the HIPAA enforcement regulation.

DOING NOTHING CAN COST A LOT!

While it is true that CEs and BAs are never 100-percent vulnerability free with HIPAA-HITECH compliance especially due to the need for change management, doing little to nothing can no longer be perceived as a low-risk/low-cost decision. In other words, the cost of doing nothing is potentially and dramatically much higher than the cost of implementing a culture of compliance (aka,-the opposite of willful neglect). And if you have a good culture of compliance within your organization you should have less risk for security incidents or breach violations.

To implement a culture of compliance, CEs and BAs need to monitor HIPAA compliance continuously and mitigate gaps, especially the high- and medium-risk gaps. The key word is continuously, which means that the process never ends.

Here are some of the elements that lead to a culture of compliance:

- Implementing written policies, procedures and standards of conduct.
- Designating a compliance officer and a compliance committee.
- Designating privacy and security officers.
- Conducting effective and on-going training and education of all of the HIPAA privacy, security, and breach requirements.
- Enforcing the HIPAA security, breach and privacy standards and implementation specifications through well-publicized disciplinary guidelines and developing policies and procedures that address sanctioning the workforce.
- Conducting periodic assessments, audits, and mitigation.
- Responding promptly to detected offenses, developing corrective action, and reporting to OCR.
- Document, document, and then document.

2013—MORE TO COME

This year, the OCR may begin auditing BAs in addition to CEs. Plus, the OCR has promised to review the 2012 audits against its audit protocols and update the protocols accordingly. We can expect to see a continual increase in the number of audits conducted each year going forward which increases the likelihood that your organization will eventually be audited.

CONCLUSION

The time to prepare for an OCR audit is now, if not yesterday. We recommend that CEs and BAs conduct internal audits based on the published OCR protocols and mitigate the gaps found. CEs and BAs may be surprised to see how difficult it is to show documented evidence of due diligence for compliance with their policies and procedures. Processes that support policies may be in place, but gathering documented evidence of the processes can be time consuming. So begin now. Two weeks is not enough time to prepare. And CEs and BAs should consider hiring an independent third party for guidance and to assess their audit readiness. **JHIM**

Gerry Blass has over 35 years of experience in healthcare IT and compliance. Gerry provides IT and compliance consulting services and software called ComplyAssistant that automates the management and documentation of healthcare compliance activities. Gerry is the President & CEO of Blass Consulting and Compliance LLC.

Susan A. Miller, JD has 40 years of professional leadership experience spanning teaching, biochemistry research and law. Since 2002, Susan has provided independent consultation and legal services to numerous healthcare entities including NIST and HHS. She has co-authored two OCR audit protocol prep-books, HIPAA Security Audit Prep Book, and HIPAA Breach & Privacy Audit Prep Book. They are published at http://www.malverngroup.com/New_Publications.html.

Blass and Miller are co-founders of HIPAA 411, a linked-in group.