POLICY AND LEGISLATION

Gerry Blass and Susan A. Miller, JD

It Is Time to Prepare for an OCR Audit

How to Prepare for HIPAA Security and HITECH Rules

By Gerry Blass and Susan A. Miller, JD

When we drive on a highway, we sometimes drive faster than the speed limit. We may be late for a meeting or we may see other drivers breaking the speed limit. We think that if they can speed, we can too. But when we see the police up ahead on the side of the road, we slow down. Why? Because we do not want to get caught speeding, pay a large fine and deal with other sanctions, such as points on our insurance. And if we get pulled over, we are really going to be late to our meeting.

Can you relate to the first paragraph? I know that I can. Our actions are sometimes related to risk. Once we see the police up ahead, we slow down in order to reduce risk of being sanctioned for a speeding violation. We also know that the level of risk and potential sanction is directly related to how fast we were driving. Ten miles per hour over the speed limit may not be sanctioned, but 20 or 30 mph over the speed limit most likely will. The potential penalty increases based on how badly we broke the speed limit.

OCR AUDITS

Covered Entities (CE) and Business Associates (BA) can now clearly see the "HIPAA police" up ahead on the "side of the road." By now most, if not all, CEs and BAs understand that they must comply with HIPAA and HITECH. And, there are other motivating factors, such as the risk of penalties and lawsuits in the event of a breach or other violations, especially when they are due to willful neglect. In addition, there are core measures in meaningful use (MU) Stage 1 (#14 for critical access and acute-care hospitals; and #15 for eligible professionals) that require information security risk analysis and mitigation. CEs cannot attest for MU Stage 1 until the MU measures are met. There is a clear financial impact. And, there is a "double whammy" for non-compliance with HIPAA from a financial standpoint. There is the risk of a penalty for non-compliance, and there also the risk of a delay in, or no attestation for, MU incentives.

GREETINGS

So what if your organization gets the "Greetings" letter from the Office of Civil Rights (OCR)? Will you have time to prepare? The answer to that question depends on what you have already done. The real answer is that you should already be prepared, and that means that you should have evidence in the form of documentation that clearly demonstrates due diligence. If you do not, or if your documentation has not been updated recently, it is time to get to work.

The OCR has not officially published the scope of their audits and it is likely that the scope will evolve. CEs and BAs, can, however, follow an audit program of reviewing what processes and documentation they have in place for every standard and implementation specification in the HIPAA Security Rule. And it is important to drill-down to the lowest level and record results.

For example, it is one thing to have a policy for a standard. It is another thing to know that the policy is operational. It is one thing to have an information contingency plan for disaster recovery and business continuity. It is another thing to know that it is operational. It is likely that the OCR will ask to see documented proof of operational audits and tests for policies, procedures, plans, etc.

How about the information Security Officer (ISO) job description? Yes, they may ask to see it and other job descriptions as well. Plus, they may ask for documented proof that the ISO's job performance is actually evaluated based on the ISO responsibilities within the job description. They may also ask your workforce members when they were last trained on HIPAA and who the ISO is. So it is important to train your work-

force and have documented proof.

Eventually the requirements of the HITECH Act of 2009 will be incorporated into the OCR audits, and the audits will be expanded to include BAs. The authors therefore conservatively recommend that CEs and BAs prepare now for an OCR audit that could cover both HIPAA Security and the HITECH Act of 2009.

The way to prepare is to assess both the HIPAA Security and HITECH rules, determine gaps, assign risk and compliance levels, mitigation action items, and manage mitigation. This process is ongoing in order to manage change. So if you have already done an assessment, the key is to make sure it is updated on a consistent basis, and that documentation exists to demonstrate due diligence.

Here is a list of potential documentation that the OCR may ask for:

- Governance (meeting agendas and minutes).
- Policies and supporting procedures and operational audits.
- Workforce training.
- Disaster recovery and business continuity plan and test results.
- Downtime procedures and test results.
- Latest ePHI vulnerability assessment.
- Latest administrative threat assessment (software, hardware, network, facilities).
- Technical risk assessments, results and mitigation (vulnerability scanning, penetration testing).
- Pro-active audits, results and mitigation.
- Access authorization, suspension, modification and termination procedures.
- Last three months terminations (OCR may do a random check of systems).
- Last three months of changes of job department and code (OCR may do a random check of systems).
- Role-based access standards (OCR may do a random check of systems).
- Incidents, results and mitigation (which of course, includes breaches and notifications).
- Workforce sanctions.
- Facility security plan and test results.
- Facility maintenance records for changes impacting information security.
- Facility and systems change management process (e.g., work group?).
- BA inventory.
- BA subcontractor inventory.
- Procedure for new BA.
- Procedure for new BA subcontractor.
- BA breach reporting process.
- Procedure for BA and physician office access termination.
- Procedure for BA subcontractor access termination.
- Password management process.
- Job descriptions (Information Security Officer).
- Inventory of systems containing ePHI.
- Inventory of systems containing protected health information.
- Hardware inventory and configuration standards.
- Other documentation that your organization may have.

Of course, the above list, although comprehensive, is just a sample of what the OCR could ask for when they conduct their audits. Again, the OCR has not published the current scope of their audits. If you have suggestions to add to the list please feel free to do so by contacting us. Our contact information is below.

CONCLUSION

Our conclusion is a simple statement: "It is time to get prepared for an OCR audit." However, the process to do so is not an easy one and it never ends. The key is to be able to show documented evidence of due diligence. **JHIM**

Disclaimer: Please note that the information within this article is not legal advice. It is for informational purposes only mainly because the OCR audit scope was not published at the time this column was written for JHIM.

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

Susan A Miller, JD has 35 years of professional leadership experience spanning teaching, biochemistry research and law. Since 2002, Miller has provided independent consultation and legal services to numerous healthcare entities, including NIST and HHS. Blass and Miller are co-founders of HIPAA 411, a LinkedIn group.