HIPAA

Gerry Blass and Susan A. Miller, JD

Audits and Evidence of Compliance

Will Your Organization Be Audited?

DESPITE THE MANY CHANGES in HIPAA (Health Insurance Portability and Accountability Act) leadership at the Office for Civil Rights (OCR, U.S. Department of Health and Human Services), the need to meet HIPAA compliance will not change, in fact, the industry has been promised that complaints, audits, and breach investigations will continue. So there is certainly a risk that your organization (if you are a covered entity [CE] or business associate [BA]) will be audited.

OCR continues to publish information about its audit program and what to expect in 2014-2015. The evaluation of the first two years of audits (Phase 1) has been completed, and OCR is now ready for the next phase. They are in the process of increasing regional staff recently evidenced by the fact that in spring 2014, they advertised for additional staff for several regional offices.

HISTORY AND STATISTICS

OCR's Overall Cause Analysis for Phase 1 is as follows[1]:

- For every finding and observation cited in the audit reports, OCR has identified a "cause."
- Most common cause (30 percent) across all entities was "entity unaware of the requirement."
- Most of these related to elements of the rules that explicitly state what a CE must do to comply.

Other causes include:

- Lack of application of sufficient resources.
- Incomplete implementation.
- Complete disregard.

In Phase 2 audits, OCR can select any CE along with a number of BAs that will be audited through the CEs. Selected CEs will receive notification and data requests in fall 2014. OCR will begin to select BAs for review in 2015.

In 2014, the plan is to audit as follows:

- Privacy: 33 health plans, 67 providers.
- Security: 45 health plans, 100 providers, and 5 clearinghouses.
- Breach Notification: 31 health plans, 65 providers, and 4 clearinghouses.

In 2015, the plan is to audit 50 BAs—all in *security*.

PREPARE

Could your organization be selected for an audit? The answer is obviously yes.

So how do you prepare? We recommend that your organization conduct a document review and organize all your HIPAA privacy, security, and breach notification policies, procedures, plans and evidence of due diligence in one place for easy access to provide to OCR. Remember that OCR only provides a two-week notice. If your organizations documentation is not organized, two weeks may not be enough time to get ready for the audit. Start with HIPAA-HITECH (Health Information Technology for Economic and Clinical Health [Act]) Security and then Breach and Privacy. Your organization should conduct and document periodic risk analysis and assessments (e.g., every year) and when there are organizational, technical, physical, administrative, and/or regulation changes. It is also important for your organization to have and show documented proof of a comprehensive workforce training program for HIPAA-HITECH rules.

We have learned from our implementation and audit practices that the following items represent strong evidence of due diligence:

- HIPAA Privacy, Security, and Breach policies, procedures and related documents, updated to the Omnibus Rule additions and changes; reviewed yearly; updated as necessary.

THE KNOWLEDGE OCR gained during Phase 1 audits will keep them focused on what they will review during Phase 2. Your organization should be prepared accordingly.

- Breach Plan, including annual table top audits.
- Training Plan, including evidence of training and training curriculum.
- Communications Plan, with meeting agendas and minutes.
- Disaster Recovery Plan, including annual table top audits.
- Audit and Monitoring Plan, reviewed annually.
- Governance documentation, with meeting agendas and minutes.
- Annual internal proactive and reactive HIPAA audits and documentation.
- Annual Security Risk Analysis/ Assessment, and documentation

It is important to keep in mind that the knowledge OCR gained during their Phase 1 audits will keep them focused on what they will review during Phase 2 audits. So your organization should be prepared accordingly. Consider conducting mock audits both internally and via an outsourced third-party organization that has the expertise to help you prepare.

And, if your organization is an eligible hospital, professional (physician), or critical access hospital in regards to the Meaningful Use (MU) rule, there are requirements for information security assessments, reviews, and updates for each stage. So from a HIPAA-HITECH Security standpoint, conducting information security risk assessments and organizing your evidence documentation will serve to prepare your organization for the potential of two audits, one by OCR and one by CMS (Centers for Medicare and Medicaid Services) for MU.

And remember that OCR and CMS auditors will not accept a simple answer to meeting standards and implementation specifications for the HIPAA-HITECH rules. They will request documented evidence of proof, as has been discussed. **JHIM**

REFERENCES

1. Sanches L. OCR Audits of HIPAA Privacy, Security, and Breach Notification, phase 2. [Presentation]. U.S. Department of Health & Human Services Office for Civil Rights. HCCA Compliance Institute. March 31, 2014. http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2014/tue/710print2.pdf. Accessed July 10, 2014.

Gerry Blass has over 35 years of experience in healthcare IT and compliance. Gerry provides IT and compliance consulting services and software 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 35 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 DHHS/CMS. Blass and Miller are co-founders of HIPAA 411, a linked-in group.