wiley

NEWSLETTER

HIPAA Phase 2 Audits Begin: Prepare but Don't Panic

April 2016

The HIPAA community has been concerned about an audit process since the HITECH mandate by Congress that the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) implement an effective audit program. Phase 1 was completed several years ago. Other than for the unfortunate few who were selected for the highly burdensome audit process, this program was uneventful and not very useful. Now, Phase 2, after several fits and starts, seems to be beginning. What do we know for sure about this process? Should covered entities and business associates be concerned? And, if not concerned, why should they be preparing for these audits even if there is only a small chance of being audited?

Phase 1

The HITECH law required OCR to conduct periodic audits of covered entities and business associates to gather information about the compliance activities of the health care industry. Phase 1—conducted in 2011 and 2012—looked at 115 covered entities. The audits of this unlucky group of 115 were extensive and burdensome. HHS gathered information about these entities, and primarily seemed to use the results to develop a "better" audit protocol going forward.

What We Know about Phase 2

- **What is actually underway now?**

Now, several years later, Phase 2 seems to be beginning. While OCR has stated that "Phase Two . . . is currently underway," what is *actually* underway at this point is the beginning of an effort to gather information about potential auditees. OCR has sent letters and emails

Practice Areas

Health Care
Privacy, Cyber & Data Governance

to various covered entities, primarily at this point to confirm or gather contact information for subsequent communications. From these initial efforts, OCR will identify "pools of covered entities and business associates that represent a wide range of health care providers, health plans, health care clearinghouses and business associates." In the second part of Phase 2, a questionnaire will be sent to the potential auditees, to gather data about the size, type and operations of each entity. This inquiry—directed initially at covered entities—also will include the identification of business associates for a subsequent stage. OCR will select its initial pool of covered entity auditees from these initial data collection efforts. HHS has made clear that OCR "will not audit entities with an open complaint investigation or that are currently undergoing a compliance review."

- **What about the substance of the audits?**

OCR has moved from the very intensive "on site" audits in Phase 1 to a Phase 2 approach dominated by "desk audits." These will involve primarily a review of policies and procedures. The first round of these desk audits will involve covered entities. A second round will address business associates. Both of these rounds are projected by OCR to be completed by the end of 2016 (although all date projections so far have been incorrect).

It also is clear that not every audit will be the same. Some audits will review the Privacy Rule, some will address the Security Rule, some may focus on the Breach Notification Rule and (apparently) some may cross these lines. The auditees "will be notified of the subject(s) of their audit in a document request letter."

The process will involve an initial email notification of "selection" as an auditee, including a request to provide documents and other data in response to a specific document request letter. *Selected companies may have only 10 business days to respond to this initial request.* For most of the "desk audits," OCR will review these documents (employing "common audit techniques"), and will share "draft findings" with the entity. Auditees will have "an opportunity to respond to these draft findings [and] their written responses will be included in the final audit report." Depending on the results of the audit or other factors, there may also be follow-up "on-site" audit visits in some situations.

- **Is this an enforcement process?**

No. OCR has made clear that the "audits are primarily a compliance improvement activity." The overall process "will enable OCR to better understand compliance efforts with particular aspects of the HIPAA Rules." In addition, "[*g*]*enerally (emphasis added)*, OCR will use the audit reports to determine what types of technical assistance should be developed and what types of corrective action would be most helpful." Also, through the audit process, "OCR will develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches."

However, throughout this process, HHS has reserved the right to turn a particular entity's audit results into a compliance investigation. "Should an audit report indicate a serious compliance issue," OCR may initiate a compliance review to further investigate.

What You Should Be Doing Now

- **Is panic appropriate?**

Definitely not. Throughout 2016, OCR will conduct desk audits of roughly 200 companies, covering a broad range of covered entities and business associates. The likelihood of being selected is small. Moreover, while there clearly will be some burden associated with providing audit responses, HHS has also made clear that its intention is that Phase 2 be less burdensome to the affected entities than Phase 1 was.

- **But what about enforcement?**

While OCR has consistently reserved its right to take enforcement action against auditees, the likelihood of this enforcement is small. The goal of this overall audit process is to gather information about the state of the industry. Enforcement clearly is not a primary purpose. OCR has hundreds (and probably thousands) of open complaints and breach reports where it can engage in enforcement investigations (and it does not have sufficient resources to move these investigations quickly). It does not need the audit process to expand this pool.

The only realistic scenario for potential enforcement would involve a situation where there is an almost complete failure of compliance activity from an auditee. If your company's response to an audit letter is "what is HIPAA," that could be a problem. Much beyond that, the risk of enforcement action is small as a result of these audits.

- **So I shouldn't even pay attention to this?**

Wrong. This is an important effort, just not one that likely will lead to specific enforcement. First, if you are selected, you will have only a short window to provide information. It will be useful to take measures now to gather information about your policies and procedures (as well as a list of your business associates and subcontractors) to be prepared to respond to an audit request.

More significantly, the steps needed to prepare for an audit are exactly the same steps that you would need to take in connection with an investigation. HHS conducts far more investigations—based on complaints, breach reports and otherwise—than it will ever conduct audits. *Your company's likelihood of facing a compliance investigation is far greater than the risk of an audit.* And, unlike the compliance audit, enforcement is a real possibility in a compliance investigation (even though OCR—for the time being—remains reasonable and understanding of sincere compliance efforts, even in investigations). So, preparing for an audit not only will prepare you for the audit—but will also prepare you for the far more likely and risky response to a compliance investigation.

- **What should we expect from the overall audit process?**

Phase 1 was not particularly helpful, at least to the health care industry. While HHS has issued certain guidance over the past few years (including some helpful documents in recent months, such as the guidance for mobile app developers on when HIPAA applies and the individual access guidance), there is little

indication that the audit program played any part in this guidance. We can expect more this time, but likely not too much.

We also can expect that the industry will be subject to some real criticism. Presumably, covered entities will do reasonably well on the Privacy Rule (although HHS remains concerned about compliance with relatively simple elements such as the individual access right). On the Security Rule, I expect more difficulty, mainly because compliance with the documentation components of the Security Rule is very hard. These Security Rule failures—from the core risk assessment element to various detailed processes—have been the failures that have resulted in enforcement activities in recent years.

The business associate community remains an enormous wild card on HIPAA compliance. This community covers an enormous range of entities, from some of the largest companies in the world to small entities and even individuals. Moreover, involvement with PHI and ePHI varies tremendously, independent of entity size (a small consulting firm might be focused on health care claims data, while an enormous business may provide services to only a handful of health care companies with very limited involvement in ePHI). Accordingly, I expect it will be difficult for HHS to draw conclusions across the board for business associates. In addition, particularly on the Security Rule, I expect business associates of virtually all stripes to fare badly in an audit process. For many companies—particularly those that are not exclusively or primarily in the health care industry—this failure may not reflect a failure of actual security, but will be a failure to meet HIPAA's process and documentation requirements. Audits aside, HHS is going to face a real challenge over the next few years concerning how to apply HIPAA's standards to enforcement investigations involving business associates.

Conclusion

So, Phase 2 is underway. It is real, and it is relatively important. It is moving, although not quickly, and will be a significant undertaking for any entity selected for the audit program. For the broader range of covered entities and business associates—the overwhelming portion of the industry that will not be selected for an audit—this process should provide a motivation to get your ducks in a row, to evaluate your HIPAA compliance activities and to be prepared in the event of a much more risky AND more likely enforcement investigation.

For more information on the Phase 2 audit process and other HIPAA developments, please contact Kirk J. Nahra.