HIPAA Audits:

A 5 Step Survival Guide for Healthcare Providers

If you ask any health IT security professional today about what keeps them up at night, a full-scale data breach is probably at the top of the list. With regulatory fines in the millions and data breach notification/mitigation costs at even higher amounts, data breaches represent one of the greatest financial risks that healthcare providers contend with today. And in light of the new HIPAA Omnibus Rules, health IT vendors now face some of the same challenges as healthcare providers.

Before the introduction of the most recent Omnibus Rules, providers used to get away with a lot. The old HIPAA rules were ex post, meaning a healthcare organization only got in trouble if something went wrong and was caught red handed. Now, Congress has added an ex ante enforcement mechanism as a side provision in HITECH which allows HHS' Office for Civil Rights ("OCR") to run periodic, randomized audits to determine an entity's compliance with HIPAA.

In 2011, the OCR spearheaded a pilot audit program and a troubling number of HIPAA noncompliance trends were uncovered. Those results encouraged the OCR to roll out a permanent HIPAA Audit. Despite the added burden of preparing for these audits, the OCR has given healthcare providers an indication of what the most important compliance areas are, in addition to guidance on how to adequately prepare for the possibility of receiving an audit.

Listed below are five crucial steps any provider can take right now to put their organization in a great position to prepare and survive such an audit.

Step One: Get Organized

Perhaps the most surprising aspect of the pilot audit program was how it tested a provider's response plan. Providers had an extraordinarily difficult time complying with the initial document request, which essentially gave compliance personnel a handful of days to submit every HIPAA plan and document on record. Of course, this was done by design – the OCR was implicitly testing a provider's response time, which could be crucial in the event of a real-life data breach.

The first thing any compliance or security professional should do is organize all HIPAA documentation on hand. This includes all policies and procedures, in addition to all PHI disclosure logs and security incident documentation. After collecting all necessary documentation, the documents should be reviewed, ensuring that everything is up to date. It seemed that many providers had the correct documentation in order, but many policies were found to be incomplete or very out of date. An incident response plan is not effective if it is 10 years out of date and the OCR has let it be known that a very out-of-date policy isn't much different than having no policy at all.

Step Two: Perform a Security Risk Assessment

In a recent Compliancy Group Webinar Series Poll (Compliancy Group Webinar Series), over 80% of providers reported that their organization had not performed a security risk assessment within the past three months. Not performing the mandated Security Rule risk assessment was one of the biggest HIPAA compliance points of failure in the OCR pilot audit program. In fact, the OCR has referenced that these risk assessments are one of the most important pieces of a HIPAA compliance program. Currently, any provider organization that fails to document annual security risk assessments will be strictly scrutinized under these coming audits.

So, what does an organization need to include in its assessment? At the most basic level, organizations must assess its potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI. It's important to note that the risk assessment requirement was designed to be scaled to the size and complexity of an organization. While a multi-facility, multi-state health system and a single physician practice all need to perform the assessment, each party can tailor the complexity of the analysis to the needs of the organization. Another important thing is to note the potential gaps and document the analysis and remediation plan in writing.

Step Three: Implement Risk Mitigation

A security risk assessment is only effective if it is acted upon. While the OCR noted that a proper risk assessment was foundational to a risk management program, it is the actual process of following up on the gap

analysis with a documented plan that truly signifies Security Rule compliance.

A number of Security Rule domains were singled out as areas in which Covered Entities faced the greatest difficulty proving compliance. In order, from highest to lowest in terms of prevalence, the following nine areas of failure were noted:

Contingency planning & backups (18% of audited entities implicated)
Media movement & destruction (14% of audited entities implicated)
Audit controls & monitoring (14% of audited entities implicated)
Access management (14% of audited entities implicated)
Risk analysis (12% of audited entities implicated)
Integrity controls (9% of audited entities implicated)
Encryption (8% of audited entities implicated)
Security incident procedures (7% of audited entities implicated)
Workstation security (4% of audited entities implicated)
If any of these domains show up as missing on the risk assessment, this will raise a question in the initial audit as well. Documenting a plan of action and following through with it will give any organization the benefit of the doubt and a clear route to follow up and correct it.

Step Four: Review Business Associate Agreements

Another major finding during the audits indicated the lack of business associate agreements between Covered Entities and their subcontractors. While industry awareness of the need for a BAA has increased ever since the passage of the HIPAA Omnibus Rule in 2013, the failure of Covered Entities to lay out PHI safekeeping procedures in the BAA is seen by the OCR as a high priority issue. A Covered Entity must be able to show that it has entered into such agreement with all of its Business Associates in order to survive an audit.

As the Omnibus Rule also made clear, Business Associates have an obligation to enter into BAAs with their subcontractors that handle PHI. As the HIPAA audits are expected to roll out to cover Business Associates, these entities must also make sure they are laying the proper foundation to survive an audit of their own.

Step Five: Include Training

A final point of emphasis in the HIPAA audits was the lack of proper workforce training. A proper HIPAA training program both educates new hires upon the start of their employment as well as provides a yearly refresher for the entire workforce thereafter. Almost as important as performing the actual yearly HIPAA awareness training is the need to document attendance to show that all necessary parties are present.

While it is not necessarily required by either HIPAA or the audits, a smart training program will also include a more detailed security awareness training specific to the organization. Such extra training not only broadens a workforce's knowledge in an increasingly important risk area, but also helps gather information that might not have been accessed otherwise. Organizations that employ this tactic frequently get workforce members to follow up with questions or initiate side conversations notifying the organization of a security concern that may only be visible at that employee's level.

Final Notes

As the government charters into new ground with the audit program, it's only natural as a compliance or security professional to fear the worst. After all, the OCR explicitly states in the pilots that the initial program was intended to be more educational to help providers "right the ship" before the full audit program goes into effect. Simply put, infractions that got a slap on the wrist during the pilot phase will now turn into fines and corrective action plans in the future. The Compliancy group can address the issues of compliance find out about our HIPAA Audit Guarantee.

The audits represent an opportunity for compliance and security professionals to ensure that they have the ear of their organization's decision makers when constructing plans to keep patient data safe. Individuals that follow the appropriate preparation steps and work with their management teams to make sure their concerns are given top priority will place their organizations in a great position to survive an OCR audit.