Your Organization Could Be Next: How to Prepare for an OCR Audit

The Office for Civil Rights (OCR), the agency tasked with oversight of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, has officially begun to implement the pilot phase of its HIPAA Privacy and Security Audit Program (Audit Program). The Audit Program, mandated by Section 13411 of the American Recovery and Reinvestment Act of 2009 (ARRA), requires OCR to periodically evaluate covered entities and business associates compliance with the HIPAA Privacy and Security Rules. To carry out this task, OCR has contracted with KPMG, a consulting company, to help design, test, and execute the pilot phase of the privacy and security compliance audit process.

So, what does this mean for you? According to OCR, KPMG is scheduled to complete 150 audits of covered entities by December 31, 2012. In selecting who to audit, OCR has clearly stated that **all** covered entities, large and small, are eligible for an audit. The audits will not only focus on organizations that have experienced breaches. Instead, OCR is evaluating a wide range of covered entities to facilitate its understanding of how different organizations implement the HIPAA Privacy and Security standards. Given that no covered entity safe, you should take proactive steps to ensure that your organization is ready to demonstrate HIPAA compliance when OCR shows up at your door. This article will outline why proactive compliance actions are necessary as well as guide you through several easy steps to survive potential OCR audits.

Cost of Non-Compliance

You may be asking yourself, why is it important to prepare for an OCR audit that may never occur? Well, there are a couple significant reasons to be prepared. First, the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of ARRA, significantly increased covered entities and business associates penalties for HIPAA non-compliance. Specifically, the HITECH Act established four categories of violations based on intent, as well as corresponding tiers of penalty amounts, that reflect increasing levels of culpability and fines for each violation, as outlined below. [1]

Intent Involved for HIPAA Violation	Penalty Amount
Violation occurring without knowledge (and where if reasonable diligence was exercised, it would not have been discovered)	$100 - $25,000 per violation
Violation due to reasonable cause (steps have been taken to remedy, not successful)	$1,000 - $50,000 per violation
Violation based on willful neglect, but corrected within 30 days of discovery	$10,000 - $50,000 per violation
Violation based on willful neglect,	$50,000 per violation

that is not corrected within 30 days of discovery	

Additionally, the HITECH Act capped the maximum penalty amount for repeat violations per year to $1.5 million. These penalty amounts, in effect as of February 2009, establish a very costly price on HIPAA non-compliance.

Second, where your organization is subject to an OCR audit and deficiencies are noted, OCR has stated that it may initiate a compliance review to further address serious problems. A compliance review could potentially lead to a Department of Justice (DOJ) investigation, which could result in a Resolution Agreement with the Department of Health and Human Services (HHS) and further monetary penalties. An example of this process is the Blue Cross Blue Shield of Tennessee (BCBST) case, which recently was settled in an agreement with HHS involving a corrective action plan and fine of $1.5 million dollars. The organization had 57 unencrypted computer hard drives containing over one million individuals' protected health information (PHI) stolen from a leased facility. The corrective action plan requires BCBST to (1) review, revise, and maintain its Privacy and Security policies and procedures; (2) regularly conduct robust trainings for all BCBST employees regarding HIPAA responsibilities; and (3) perform monitor reviews to ensure compliance with the corrective action plan.[2]

Lastly, failure to comply with the HIPAA Privacy and Security Rules can result in irreparable damage to the organization's reputation. Under the HITECH Act, covered entities are required to report breaches of PHI to HHS. Specifically, for breaches involving 500 or more individuals in the same state or jurisdiction, the covered entity not only has to report the breach to HHS but also notify a major media outlet. The negative publicity can take years, if possible, to revert. Further, the covered entity will be faced with the challenge of restoring patients' confidence and trust of the organization.

Questions to Ask and Answer: Are You Ready?

In order to demonstrate active HIPAA Privacy and Security compliance, providers should be able to answer the following questions.

1. **Are our HIPAA policies and procedures up to date and effective?**

All covered entities should have organizational policies and procedures that address each addressable requirement in the HIPAA Privacy and Security regulations. These HIPAA policies and procedures should be updated on a timely basis to reflect any regulatory or organizational changes. For example, your organization should have already created a *Breach Notification* policy to address the changes outlined in the HITECH Act, enacted as part of ARRA. Further, when the final HITECH Act regulations are published later this year, several of your organization's HIPAA policies and procedures will need to be updated. Organizations should also be monitoring employee compliance with HIPAA regulations to ensure that the policies and procedures in place effectively guide employees to correctly follow required HIPAA practices.

2. Is our HIPAA training effective and up to date? How do you know?

HIPAA requires all covered entities to deliver HIPAA training to its employees. These training presentations should be updated on a regularly basis to reflect regulatory or organizational changes. Additionally, organizations should have a system in place that evidence training completion, as well as procedures to ensure that trainings are delivered and attended in accordance with internal policies and procedures. Further, organizations should have evidence to substantiate that the trainings delivered are effective in providing employees with the information necessary to comply with HIPAA. Suggested ways to measure effectiveness include either testing or surveying employees, upon completion of training or periodically, to ensure that the training content is retained.

3. Have we conducted a risk assessment?

The HIPAA Security Rule Administrative Safeguards provisions require covered entities to perform a risk assessment as part of their security management processes. When analyzing potential risks to the security of PHI, organizations should (1) evaluate each risk's likelihood and impact; (2) implement appropriate security measures to address identified risks; and (3) document the selected security measures, including an explanation of the reasoning for selection. Any corrective action taken by an organization as a result of the risk assessment findings should be monitored to completion and documented. As risk assessment is an ongoing process, organizations should update their risk analysis, at least annually, to ensure that risks are appropriately identified, remediated and monitored. Additionally, internal controls and security measures used should be regularly monitored and evaluated to ensure that PHI is appropriately and effectively protected.

4. Do we have an ongoing auditing and monitoring programs for HIPAA Privacy and Security?

Organizations should be monitoring its HIPAA Privacy and Security compliance on an ongoing basis. Compliance Officers, in conjunction with the HIPAA Privacy and Security Officers, should be monitoring completion of HIPAA education, as well as detecting and investigating potential HIPAA incidents occurring during daily operations through the Hotline and any Human Resources and patient complaints. Additionally, there should be several HIPAA items included in the organization's annual audit plan, specifically focusing on ensuring that patient records are accessed and disclosed appropriately and that internal controls are effectively securing PHI.

5. Have we had any breaches?

Hopefully, you have not. However, regardless of whether a breach has occurred, there should be a well established documented process that explains how a potential breach scenario is handled. Additionally, where a breach does occur, special attention should be paid to ensure that

appropriate documentation is maintained to outline each step of the process, including the procedures used to notify all appropriate parties.

Four Easy Steps to Take to Prepare for an OCR Audit

It is not too late to start preparing for the OCR audits. Here is a quick list of steps you can take to ensure that your organization is on track.

- **Step 1: Prepare an Audit Response Team.** A key component in surviving an audit is to ensure that the organization responds to government's requests appropriately. An Audit Response Team can help to organize and facilitate a timely response to any OCR requests. When developing an Audit Response Team, be sure that the team consists of the necessary subject matter experts to promptly gather documents and address inquiries for the audit. At a minimum, the Audit Response Team should include the Compliance Officer, Privacy Officer, Security Officer, and Health Information Management representation.
- **Step 2: Audit your organization's HIPAA documentation.** OCR has instructed KPMG to review covered entities' HIPAA documents as part of the audit. As such, covered entities should evaluate their HIPAA policies and procedures and verify that the documentation is organized and current. Covered entities must ensure that their policies and procedures are in final form, i.e., no "track changes" and are easily accessible. In addition, you should review your organization's complaint logs, investigation work papers, corrective action plans, training materials, and training attendance logs and ensure that records are complete and fully reflect the organization's efforts to be HIPAA compliant.
- **Step 3. Conduct a Risk Assessment.** If you have not already done so, you **must** conduct a risk assessment. A risk assessment is not only a requirement under the HIPAA Security Rule, but also is an effective tool in identifying gaps and weaknesses in the organization's internal controls. The risk assessment process forces an organization to pinpoint and manage their risks which are all pro-active activities that evidences an organization's will to be compliant.
- **Step 4. Identify all Business Associates.** OCR's initial announcement of its audit plans indicated that both covered entities and business associates will be subject for review. However, OCR later announced that the audits will focus on covered entities and "business associates will be included in future audits."[3] Therefore, given the complexity of business associates, covered entities are strongly encouraged "to get a handle" on their business associates sooner rather than later. Organizations should identify their business associates and review written agreements to ensure that HIPAA compliant requirements are included in the business associates' contracts. Further, organizations should periodically assess and document business associates compliance with the HIPAA Privacy and Security Rules.

Additional Solutions to Consider

If all the steps listed above are not feasible or difficult to fulfill, there are other options to help your organization demonstrate HIPAA compliance. Notably, organizations should consider the following:

- **Outsourced Privacy and/or Security Officer(s).** Part of the success in surviving an OCR audit, is having the Privacy and Security Officer(s) actively involved. Thus, it is imperative, as well as a HIPAA requirement, for a covered entity to appoint a Privacy and Security Officer(s) to oversee the privacy and security programs. If an organization does not have personnel who can fully meet the responsibilities of the Privacy and Security Officer(s), the organization should seriously consider outsourcing the role to meet federal requirements and enhance an organization's HIPAA compliance.
- **Request an External or Third-party Risk Assessment.** As mentioned above, risk assessment is an effective tool to identify and manage risks. Covered entities can conduct internal risk assessments; however, an external risk assessment can provide valuable insight for the organization. An external risk assessment can identify risks that may otherwise been concealed or overlooked during an internal risk assessment.
- **Purchase Compliance Tools.** Health care organizations are under greater scrutiny today than ever before. Moreover, health care organizations are pulled in various directions and must monitor and comply with several federal and state requirements. As such, organizations need easy access tools to stay complaint. Covered entities should consider purchasing compliance tools such as policies and procedures, compliance training, electronic contract management software to facilitate the organization's compliance efforts.

Although, the OCR's Audit Program brings HIPAA to the forefront, HIPAA compliance is not new and will continue to pose challenges for covered entities and their business associates. Organizations must be aware that the HIPAA Privacy and Security Rules have been enacted for several years and the government expects you to have established policies and procedures to comply with the law. Organizations cannot afford to do nothing. HIPAA compliance is a must. Thus, organizations are strongly encouraged to implement the best practices as outlined in this article independently or seek external assistance.

---

[1] HIPAA Administrative Simplification: Enforcement, Interim Final Rule. 74 Fed. Reg. 209, 56123, 56125 (Oct. 30, 2009).

[2] Department of Health and Human Services. "HHS Settles HIPAA case with BCBST for $1.5 million." Press Release. 13 Mar. 2012. http://www.hhs.gov/news/press/2012pres/03/20120313a.html.

[3]Department of Health and Human Services Office for Civil Rights. " HIPAA Privacy and Security Audit Program." Accessed on 31 May 2012. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html>.