HIPAA

Gerry Blass and Susan A. Miller, JD

The Top Ten Things Your Organization Should Be Doing to Pass an Audit and Reduce Risk of a Breach

Imagine trying to come up with the top ten things our planet should do to decrease vulnerabilities and threats. Looking at earth from 30,000 feet can make that seem easier to do. But if we zoom in to the details we could probably come up with hundreds of things to consider. The same is true with health information privacy and security. To come up with what we consider to be the top ten things to do to pass an Office for Civil Rights (OCR) audits and reduce risk of unauthorized access to your protected health information (PHI), we had to zoom out and look at what we have observed over the past several years from a very high level. Our top ten things to do are not listed in any particular order. Keep in mind that our top ten today will most likely change very soon and at least year to year. Here they are:

1. Be a functional organization with information privacy and security (via mandates, oversight, change management, resourcing, and empowering the information security officer or ISO).

Functional organizations have implemented executive mandates for compliance and adequate budgets for both human and funding resources. The authors have heard a well-respected Compliance Officer in New Jersey state "The cost of compliance is potentially much less than the cost of an incident such as a breach." All of us who have read about the recent and ongoing breach incidents can agree with that comment.

It is interesting that we are also starting to hear about and see ISOs reporting outside of Information Technology (IT). This makes sense because the ISO needs to be able to audit the IT controls and give an unbiased report to senior management. Other areas to consider for the ISO to participate with or at least report to include compliance, legal, audit, and risk.

The goal is to create an ever-changing culture of compliance that prepares organizations for government audits and reduces the risks of adverse events such as a breach of their PHI. A key component of oversight is change management. The reason why compliance activities must be done periodically is due to change, to regulations, administrative, physical, and technical risks and vulnerabilities, and organizational factors, such as M&A, policies and procedures, new facilities, new technology, application updates, and more.

We have included change management as number one, but consider it to be part of and a strong requirement for every item on our list.

2. Documentation

The basic requirement for any compliance program is documentation, including policies and procedures, risk assessments, plans (e.g., disaster recovery plans, facility security plans, etc.), and other evidence documentation that proves operational compliance. The OCR will request documentation of both internal vulnerability scanning and external penetration testing during their audit.

All documentation should be reviewed on a periodic basis, at least annually. Disaster recovery, business continuity, and procedures should be tested each year as well. The tests should be both tabletop and actual controlled testing of offsite backup and restore locations. Departmental downtime procedures should be tabletop tested at least annually, and there is normally actual downtime that results in actual testing. Breach response plans should also undergo tabletop testing.

Facility walk thru audits should be documented while referencing the facility security plan. Any gaps should be reviewed and included in the risk mitigation plan. Remember that the "acid test" for determining physical security issues is this: if you can see or access PHI in an unauthorized manner (e.g., workstation monitor containing PHI is in full public view), there is an issue to be resolved before it turns into an incident.

Documentation is your first line of defense when the OCR comes calling, whether it is for an investigation or audit.

3. Risk Assessments (RA)

Risk assessments (RA) should be done at least annually and always when a change could result in a new vulnerability that increases the risk of unauthorized access to your PHI. As mentioned above, the change could be administrative, physical, technical, or organizational. It could also be due to a change in the regulations. RA is a general term but should include: A review of the entire HIPAA security rule, technical security testing (internal and external), an administrative threat assessment, a PHI vulnerability assessment, physical facility walk thru audits, a cyber security assessment (can be part of the technical testing), and random workforce interviews to gauge their competency for high level HIPAA knowledge, which is something that may be done during a real OCR audit.

4. Risk Management (RM)

The authors have witnessed covered entities and business associates who outsource a risk assessment and then make very little progress or sometimes no progress in managing the identified risk. The good work that was done during the assessment is no longer evidence of due diligence, but rather, possible evidence of willful neglect. This is another reason for a strong oversight committee that meets on a regular basis to review progress with risk mitigation. And it goes back to proper funding. Dedicated resources and funding for risk management is the key to success. Risk should be managed in tiers, focusing first on high risk, then medium. Low risk should also be reviewed to confirm that it is truly low, and whether any mitigation is required. RM must follow every RA activity, and the results must be documented so that your organization has evidence of due diligence rather than willful neglect.

5. Yearly Compliance Audit

Since President Obama signed the American Recovery and Reinvestment Act (ARRA) in 2009, the OCR has been out saying at national meetings and on webinars that all covered entities must do a

Insulin pumps, pacemakers and other such devices have computer chips in them that collect medical information of an individual patient, so they may need to meet the HIPAA privacy and security requirements.

yearly HIPAA compliance audit. This can be done in-house, or your can invite an external consultant to assist you. With the advent of the Omnibus Final Rule in January 2013, the OCR has added the business associates to this requirement of a yearly internal compliance audit.

You can do your yearly RA as the first step in this yearly audit. Additionally, this self-audit permits you to know and keep all the HIPAA documentation in one place, one electronic file, or to have an inventory of where and who keeps the documentation.

One of your authors had a client go through an OCR audit in round 1 and another client in round 2, and they both have stated that without such knowledge of where all the documentation is may cost you up to 200 - 300 man hours to find and validate your organization's current HIPAA documentation.

6. mHealth

mHealth is an abbreviation for mobile health, a term used for the practice of medicine and public health supported by mobile devices.

The real question is what HIPAA privacy and security requirements need to be in place for mobile communication tools, telehealth and wearable devices, and what a breach is in each of these areas. For example, does a 'FitBIt' need to meet the HIPAA privacy and security requirements? It does collect what would be PHI if the device was provided to you by a HIPAA covered entity or business associate. Insulin pumps, pacemakers and other such devices have computer chips in them that collect medical information of an individual patient, so they may need to meet the HIPAA privacy and security requirements.

Right now the OCR is very concerned about mobile devices and wants them included in any RA, but it makes sense to include all telehealth services, mobile clinical tools that collect PHI, and any wearables provided by your office or hospital in your yearly RA. All these areas also need to be part of your enterprise training.

7. Clouds, Offshore, and Remote Access

Cloud, offshore work, and remote access are additional areas where there is blurring in healthcare. Today, cloud is often being used unknowingly, and creative doctors and other staff are creating security risks and vulnerabilities of which you have no knowledge until you do an audit or have an event.

Offshore work and remote access are in a category by themselves. For offshore work you need a good policy and business associate agreement that includes a cybersecurity insurance provision and a provision where the offshore entity will submit to a court's jurisdiction even if they have no USA parent organization. We suggest that the insurance be with an American insurance company that you can reach if the offshore entity refuses to submit to state or federal court jurisdiction.

Another thing to do for both offshore and remote access onshore workers is to devise a survey to make sure they are not working in areas that are vulnerable to unauthorized access. Again, a strong set of polices and periodic audits must be in place to demonstrate evidence of due diligence.

Include all of the above in ongoing risk assessments and mitigation.

8. Business Associate (BA) Management

The first step in BA Management is to develop a BA inventory and risk rate it by tiers (high, medium, and low).

Next, make sure your BA agreement template is up to date according to the Omnibus final rule, as well as your business needs.

Since many covered entities, and business associates, have hundreds of BAs, the process to assess them becomes a major project. The best time to assess them is pre-contract. Depending on the risk tier and the type of BA, there are key questions that should be asked. The authors recommend the CEs use an electronic central repository to manage the tasking and management of BA compliance, and for review and follow-up. One assessment question / request can be to attach an executed BAA. Keeping all answers and evidence documentation organized in one electronic repository for each BA is a good way to demonstrate due diligence and to learn where your organization could be at risk for a breach caused by a BA due to weak controls over your protected health information.

9. Cybersecurity Controls and Insurance

Cybersecurity is security applied to computers, computer networks, and the data stored and transmitted over them. Recent cyber attacks have made the headlines due to the large number of individuals involved in the breaches, most in the millions. Vendors who market intrusion detection solutions are striving for advanced algorithms that better detect potential hacks. It is extremely important for CEs and BAs to know all potential locations that could be vulnerable to a cyber attack, and determine the risk mitigation plan. The authors recommend that CEs and BAs outsource their Cybersecurity RA and RM to expert consulting companies who are up-to-date on the latest intrusion detection technology. CEs and BAs should also refer to the National Institute for Standards in Technology (NIST) for reference information. Finally, CEs and BAs should consider adding cybersecurity insurance for additional protection due to the potentially large costs of breaches, especially the typically large breaches caused by a cyber hack.

10. Comprehensive Training

Workforce training should be comprehensive since one of the biggest risks of unauthorized access and / or use of your organization's PHI is internal, namely the workforce. There have been a number of incidents due to accidental or intentional violations. In order to show due diligence and to be able to apply sanctions to violations, your workforce must understand your policies and procedures. Training normally begins during orientation for new workforce members. In addition, there should be periodic mandated training and manual or electronic testing to determine competency. Low competency results should be remediated immediately via focused training. The authors believe that the most effective training is in the form of reminders. One very impressive way to deliver the reminders is via workstation screensavers. They can be set up to continually scroll information privacy and security reminders. Not only is it the best way to deliver the reminders, but it is also very impressive when an auditor sees the scrolling messages on every workstation. This is a simple solution with a major positive impact.

CONCLUSION

Remember, full HIPAA compliance does not necessarily mean NO security incidents or breaches. Your HIPAA compliance needs to be both broad and deep! *Remember*, you need to have constant compliance that is backed up by yearly training, a yearly RA, and a yearly HIPAA compliance audit. *Plus*, your RA must include the new technologies that you introduce to your organization ... if you are you thinking about virtualization or hyperconvergance make sure they are on your tick list for your next RA! **JHIM**

Gerry Blass is the President and CEO of ComplyAssistant. Gerry has over 35 years of experience in healthcare IT and compliance. Gerry provides IT and compliance consulting services and software (also called ComplyAssistant) that automate the management and documentation of healthcare compliance activities. To learn more visit www.complyassistant.com.

Susan A Miller, JD, has 40 years of professional leadership experience spanning college teaching, biochemistry research and law. Since 2002, Susan has provided independent consulting and legal services to numerous healthcare entities including NIST, CMS and OCR. She is the author and content manager of the NIST HIPAA Security Toolkit. She has co-authored two OCR audit protocol prep-books, HIPAA Security Audit Prep Book, and HIPAA Breach & Privacy Audit Prep Book You may reach her at TMSAM@aol.com.

They are published at http://www.malverngroup.com/New_Publications.html.
Blass and Miller are co-founders of HIPAA 411, a LinkedIn group.