What is the Government looking for in a HIPAA Audit?

As a Services Provider, OMG strives to stay ahead of potential issues that will affect our clients either financially, legally or both. One area of concern that is front and center for Healthcare providers is HIPAA compliance. With the recent "hacks" of personal data, corporate websites, etc., maintaining a secure environment for Personal Health Information (PHI) is absolutely critical. OMG understands that our clients expect us to ensure that any PHI or Laboratory Samples are handled via the guidelines set forth by the Health and Human Services Department. This article talks about the importance of being prepared for a HIPAA audit. Why is this important? The government is funding many of their programs that have been cut or have reduced revenue generation through the fines issued for HIPAA violations.

As a refresher, HIPAA is governed by the Office of Civil Rights (OCR) within the Office of Health and Human Services (OHHS). The HIPAA Privacy Rule has been in place since 1996. The HIPAA Security Rule took effect in 2003, however, it wasn't until the Affordable Care Act (ACA) created the HIPAA Omnibus Rule that audits began in earnest.

- When the HIPAA Omnibus Rule went into effect on March 23, 2013, the intent was to make Business Associates (BA's) more accountable for the protection of the data they were managing on behalf of Covered Entities (CE's) such as hospitals or health plans.
- Prior to this, BA's were only liable for whatever was put into a Business Associates Agreement (BAA) by the CE, and even then that liability was restricted to any civil action that may be taken by the CE.
- However, the Omnibus Rule extended the same federal provisions to BA's that had previously been restricted to CE's, meaning that whether a business associate signed a BAA or not, they were federally required to operate in accordance with the Security, Privacy and Breach Notification rules. Failure to do so could result in federal penalties of up to $1.5 million per breach type, and even criminal prosecution.

This change was driven by the fact that an increasing percentage of healthcare data is being managed by BA's such as health IT vendors and other service vendors. While Covered Entities' still account for the majority of breach incidents, Business Associates' are responsible for most of the records breached.

- It is currently estimated there are 5 million Business Associates dealing with Personal Health Information (PHI) on a daily basis.
- Prior to now, patients could not sue the CE's/BA's for HIPAA violations, however, beginning in 2015, patients will be allowed to sue for breach of their PHI and receive compensation, this is in addition to the fines levied by the OCR.
- Soon attorneys will be involved, there will be more audits and a seemingly innocuous comment could spur an audit being initiated.
- OCR outsources the majority of HIPAA audits – the auditors are the "judge, jury and executioner" – each breach of HIPAA has a typical fine of $50,000.
- For every dollar the OCR spends on audit costs, they receive twenty dollars back in fines.
- The money brought in from fines is being used to fund Medicaid, Medicare and "meaningful use programs. To get an indication of how the OCR has increased the number of audits per year with the resulting increase in revenue from fines, see the table below:

Calendar Year	Number of HIPAA Breaches reported	Amount in Fines the OCR has collected	Notes
2012	9,500	$4,000,000	Patients can't sue for HIPAA violation.
2013	19,000	$6,500,00	Omnibus Rule goes into effect – now penalizes Business Associates.
2014*	24,000	$11,000	Patients can sue for HIPAA violation, but fines go to the OCR.
2015	TBD	TBD	Patients can sue for HIPAA violations and receive compensation.

*Through July of 2014 only

So "what do we do to avoid a HIPAA breach? Breaches happen most often by the internal staff. Conduct a walk through and see what is out of compliance at a glance? There are 46 HIPAA specifications that each organization must comply with. The following are just a few of the areas that are frequently in breach:

1. Sharing passwords
2. Too many Administrative passwords
3. Passwords not complex or updated
4. Bad back-up policies or non-enforced
5. No "auto log-off" or screen saver
6. Paper based PHI visible or not in a secured area
7. Verbal discussion of PHI that can be overheard
8. IT Server not in a secured area
9. Computer screens not physically adequate
10. No TV or ambient noise
11. No secure window at check-in
12. Staff not informed during Audit interviews
13. Bad IT – encryption not used
14. Mannerisms and voice levels during Audit interviews
15. No talking about PHI before entering an Exam Room
16. Lack of an Alarm System
17. Outsourced vendors/services have easy access for non-managed areas
18. Port 3389 should never be open to public access
19. Remote access must be monitored
20. Historical access – who can still get in to the system

All companies should review the National Institute for Standards and Technology to ensure they are looking at each of the HIPAA specifications and understanding them. Small healthcare providers have more compliance issues than larger ones. Business Associates and healthcare providers have many more issues than Clearing Houses and Insurance plans. What else can companies do? Call an expert like OMG who is current with Federal legislation regarding HIPAA violations, we will take a look at your current operations and help you get the documentation and materials prepared so that you will be ready should the OCR send you a HIPAA Audit notification. Compliance is the key and OMG will ensure that your organization will be ready to pass a HIPAA audit! Call today at 800.207.4807 or e-mail info@omgservices.com. Let us help you be ready!