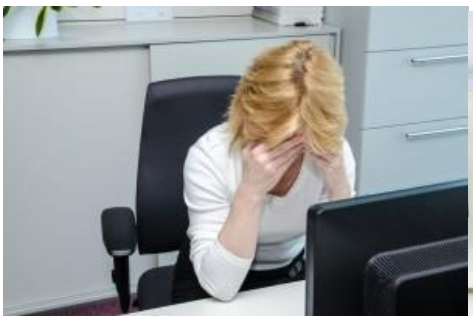
SEMEL CONSULTING **HIPAA Brief**

Imagine Your Life if you Fail a HIPAA Audit (or worse…)

Prepare Now Because of Short Response Times




Imagine your life if your organization fails a federal HIPAA audit.
Imagine giving back your Meaningful Use money and having your Medicare payments reduced.
Imagine having the Federal Trade Commission put you on a 20-year monitored compliance program.
Imagine ALL of your patients suing you for malpractice, *at the same time*.
Imagine your day. Imagine the impact on your career. Imagine all the people who will be hurt.

Last week those of us attending the HIPAA Security conference in Washington heard clear warnings from the Office for Civil Rights (OCR) leaders that should make everyone who has to comply with HIPAA take notice.

Audits Coming Very Soon

1. While audits have been discussed for a long time, they are imminent. 1,200 letters will be going out shortly. 1,200 out of the entire health care industry means the odds of you getting a letter are low. But if you do, the impact can be very high.
2. If you receive a letter you will have only 10 – 14 days to provide the requested documentation. That isn't enough time to overcome years of HIPAA neglect, particularly with the Security Rule protecting data.
3. A contractor has been hired to conduct the audits, and the OCR has been hiring attorneys. They aren't there to help you.
4. The audits will likely focus on areas that were identified as common weaknesses in the 2012 test audits – no security risk analysis, not addressing risks, unencrypted data, and lack of effective policies and procedures.
5. Small practices will be targeted. In 2012, many smaller practices were found to be lacking in their compliance efforts. The new audits are likely to be skewed towards small medical practices and hospitals, not large health systems.
6. Are you confident your Business Associates won't cause you to fail the audit? When a Covered Entity gets audited the OCR will now examine their Business Associates. In our experience Business Associates are often clueless about their HIPAA responsibilities, beyond signing Business Associate Agreements. Have your Business Associates complied based on the 2013 HIPAA changes?
7. Patients' rights to their records, especially the new requirements for electronic records, are not being followed by many HIPAA Covered Entities. This is a Hot Button with the OCR which is charged with protecting the rights of patients.
8. Haven't had a HIPAA incident? Most likely you have, and either don't recognize them or aren't giving them serious consideration. Data breach notification requirements have changed since 2009, and OCR wants to know if you have a clear policy and practice in place for notifications.

Encryption

Encryption was probably mentioned more than 50 times. No kidding.
At the conference, Jocelyn Samuels, the Director of the OCR, announced a $ 750,000 settlement with a small cancer practice that had a bag that contained an unencrypted laptop and unencrypted backup media stolen from an employee's car.

Deven McGraw, the new Deputy Director of the OCR for Patient Privacy, said, "*The bigger problem with breaches involving lost and stolen unencrypted devices is that they are often a tip off for OCR that an organization has other more serious HIPAA compliance issues – particularly the failure to conduct a risk analysis that's followed up by actually mitigating identified risks*." This is more than a subtle hint.

Other speakers stressed that encryption not only protects patient data, but it protects the Covered Entity against having to report a lost or stolen device. Encryption is much less expensive than HIPAA penalties. Check out this article **HIPAA Enforcer Losing Patience on Encryption** for more details.

So What Can You Do? PREPARE NOW.

1. Quickly obtain a thorough and accurate Security Risk Analysis, not a 'checklist overview' that will miss critical issues. Should you do your own? The US Dept. of Health & Human Services says, *"…doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.*" This is coming from the agency that does compliance reviews and has failed many practices that have done their own risk analyses. As the famed oil well firefighter Red Adair said, "*If you think it's expensive to hire a professional to do the job, wait until you hire an amateur.*"
2. Fix the problems identified in the Security Risk Analysis. HIPAA requires Risk Management for both security and compliance. Years of neglect may be expensive to correct. Encryption is an obvious starting point.
3. Have an expert review your Notice of Privacy Practices and your Business Associate Agreements to make sure they are current and properly implemented. And your Data Breach Notification policies and procedures.
4. Contact Semel Consulting. We'll do a risk analysis, help you fix your risks, implement effective policies and procedures, and help you with any HIPAA questions or incidents. We have helped many organizations including small medical practices, large clinics, surgery centers, hospitals, nursing home chains, home health care, health plans, and many Business Associates.
5. Be on the lookout for the audit letter. It won't be good if someone who opens your mail misses the letter and you miss the deadline. Especially when you have made the efforts to comply.

Now imagine your life when you pass a federal HIPAA audit.

Meaningful Use

To qualify for Meaningful Use incentive payments you need a Security Risk Analysis AND you need to remediate your risks before or during your reporting period. We just signed a client that has returned all of their Meaningful Use payments, and faces reduced Medicare reimbursements moving forward. Falsely attesting when you haven't complied can be penalized through the False Claims Act, requiring a payment of three times what you received, or can be prosecuted as Medicare fraud.

Federal Trade Commission

The FTC treats patients as consumers and is penalizing organizations that have data breaches. The FTC doesn't have the same financial and penalty restrictions as the OCR. They caused a medical lab to shut down. They placed a Business Associate on a 20-year monitored compliance program. You should be more afraid of the FTC than OCR if you have a data breach.

Malpractice

HIPAA has been used successfully as a Standard of Care in a Malpractice suit. The jury awarded $ 1.8 million saying that every HIPAA Covered Entity *knows it has to comply with HIPAA,* just like making sure doctors wash their hands and wear gloves. If you have a breach of your patient records, it is now possible for an attorney to sue you for malpractice on behalf of all your patients.

About Semel Consulting

We are experts in HIPAA compliance, many other federal, state, and industry regulations, and Information Technology. Our founder has been the Chief Information Officer (CIO) for a hospital and a K-12 school district. He was the Chief Operating Officer for an online backup company, and has owned IT businesses for 30 years. He is certified in HIPAA, other regulations, and Business Continuity planning, and is a nationally known speaker, trainer, and writer. We have done HIPAA compliance projects since 2003. We work with medical practices, hospitals, health plans, and many types of Business Associates.

We don't stop with a HIPAA Security Risk Analysis. Our HIPAA SOS Service includes the risk analysis, plus a HIPAA compliance assessment that includes the HIPAA Privacy, Security, and Data Breach rules. We work with you to comply with other federal and state laws that affect you.

We treat you like you treat patients – we diagnose your problems and develop a treatment plan, then we treat you until you are well and put you on a wellness plan to keep you secure and compliant.

HIPAA SOS includes HIPAA Security Rule Policies & Procedures, checklists, cyber security training for your staff, a Certified HIPAA Security Professional (CHSP) certification class for you (or your designee,) and ongoing consulting for a year.

We will assist you if you are audited. If you have a HIPAA incident or data breach, we will assist you with complying with the notification and reporting requirements. We aren't attorneys, but can recommend some that focus on HIPAA and other healthcare issues. We aren't selling IT products or services, so our assessment is to help you, not to sell you something. Check out our website www.semelconsulting.com/testimonials to see what our clients are saying.