SEMEL CONSULTING HIPAA Brief www.semelconsulting.com

HIPAA Compliance Tech Tips updated October, 2016

HIPAA Compliance Tech Tips

Technical Requirements You May Not Understand

HIPAA Compliance can be a mystery. HIPAA is vague so it can be flexible and scalable. Guidance refers to other government guidance. When you dig deep and try to understand the tasks and procedures you need to protect electronic data you are likely to encounter technical terms—and IT buzzwords— that may be confusing. Here are some tips you can use to ensure that your technology foundation is secure enough to support HIPAA compliance. Remember that HIPAA compliance is a fundamental requirement for medical providers to earn and keep their Meaningful Use incentive money. IT departments and Managed Service Providers have to apply compliant security controls and properly document them.

Overview

HIPAA protects any combination of something that can identify a patient along with anything related to their diagnosis or treatment, in any form– written, verbal, or electronic. The Security Rule provides a framework for protecting electronic Protected Health Information (ePHI.) HIPAA compliance was designed to be flexible enough to apply to health care organizations of all kinds and sizes. Some HIPAA Security Rule requirements are Required and others Addressable. *Addressable* specifications are sometimes confused as being Optional, which is not true. The US Department of Health & Human Services says *"**a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative.**"*

Our advice if you want to achieve HIPAA Compliance is to assume that everything in the Security Rule is required, and you should set a very high bar if you decide not to implement an Addressable item. If you believe that an Addressable specification is not reasonable or appropriate, you must document your decision and hope it stands up to a HIPAA audit or data breach investigation.

Speak Geek?

If you don't understand the terms you should contact an IT Managed Services provider to help you evaluate your network. When it comes to surviving a HIPAA audit or data breach investigation, you need an IT professional. Like the specialists doctors refer patients to, and the tests that they order to see what is happening under a patient's skin, your technology must be evaluated by someone with the proper skills and experience, who must look deep into your network to identify its strengths and weaknesses. Make sure they understand the HIPAA compliance requirements you face. One way is to ask if they employ a Certified HIPAA Security Professional.

Business-class operating system

When you turn on a computer the first thing you encounter is the operating system, usually Windows or Macintosh. What you may not know is that there are different versions, some with little or no security built in to save costs and keep prices low. Consumer versions of Windows and Macintosh operating systems do not protect the files stored on the device, do not allow you to securely connect to a network, and not include data encryption. You need to have a business-class version of the operating system and make sure it is properly set up to protect stored data and to securely join a network.

This means you should not be buying computers for your network from retail stores that offer low-cost consumer products. Make sure you achieve HIPAA compliance by purchasing professional models with business-class security. Also, Windows XP lost its security updates in April, 2014, which means that XP computers and medical instruments with imbedded XP computers are no longer HIPAA compliant and are a high risk of being breached. Office 2003 has been retired and carries the same risks. Microsoft publishes its software lifecycles so it is easy to see that Windows 7 will lose its security patches and updates in 2020.

Business-class E-mail & Text Messaging

Webmail services like G-mail, Hotmail, Yahoo!, and those provided by your Internet Service Provider (ISP) are not secure enough to send Protected Health Information (PHI.) These services do not provide end-to-end e-mail security, and the vendors will not sign Business Associate Agreements. A small medical practice paid a $ 100,000 fine for using webmail and an online calendar for PHI. Another recently paid $ 2.7 million for sharing PHI with a cloud vendor that is not HIPAA-compliant and will not sign a Business Associate Agreement, and also for using unsecure e-mail for PHI.

For HIPAA compliance you need to use a secure e-mail solution provided by a secure server you own; a secure Cloud e-mail or encryption service from a vendor that will sign a Business Associate Agreement; or by using the secure communications tools included in your certified Electronic Health Record (EHR) system. Faxes are OK between practices and pharmacies, unless your system converts the fax into an e-mail, which cannot be sent to a webmail account. TEXTING USING THE CELL CARRIER'S SYSTEMS IS NOT SECURE OR HIPAA-COMPLIANT. NEVER TEXT PATIENT INFO AND MAKE SURE YOUR ANSWERING SERVICE IS NOT TEXTING.

Secure Network Infrastructure
There are two ways to set up a Windows network, a Workgroup or a Domain. A peer-to-peer Workgroup is a loosely connected group of workstations. A Domain is centrally managed and includes security features. You cannot be compliant with many HIPAA requirements like Information System Activity Review, Unique User Identification, Audit Controls, and Person or Entity Authentication in a Workgroup. You need a Domain. You may need to purchase a server, convert your existing server into a Domain Controller, or create a secure network in the Cloud. A Workgroup is a deal-breaker if you have any protected data anywhere other than your certified EHR system unless you have another way to log access and retain logs for six years. Keep in mind all the old files you still must retain.

Encryption
While encryption is Addressable for HIPAA compliance, if you don't have it and a device containing health information is lost or stolen, you must notify patients and report the loss to the federal government for an investigation. If a lost or stolen device is encrypted you do not have to notify patients or the government. You can purchase encryption for almost every type of computer. You can even purchase laptops that automatically self-encrypt when you turn them off or close the lid. In 2012 a state health department paid a $ 1.7 million penalty for a lost unencrypted hard drive. A hospital paid a $ 1.5 million fine for a lost unencrypted laptop. In 2014 a health care provider paid $ 1.725 million for losing an unencrypted laptop. Encryption costs a lot less than patient notification and fines.

Passwords and Automatic Logoff
Yes, I know they are inconvenient and annoying. However, HIPAA compliance requires audit trails to identify which user accessed patient records. For this reason individual users must log on and off by themselves, and not allow sharing of passwords or piggy-backing multiple users during a single session. Automatic logoff is Addressable, but the alternative choices are expensive and very inconvenient. While you do not have to use Automatic Logoff, the alternative is to NEVER (ever) allow a patient in the room with an unlocked computer. You would either have to have the doctor wait in an examining room for each patient to arrive and stay until they leave, or hire additional staff to NEVER (ever) leave a patient in a room with an unlocked computer. There are ways to make logging back on more convenient, like fingerprint readers and proximity cards. Accept the facts that you need to have each user log in and out, and that automatic logoff must be used. Like airport security and searches on the way into ball games and concerts, Security is a new way of life.

Firewall
Your network is connected to the Internet by a router or a firewall. A router directs traffic between two networks—your internal network and the Internet. A firewall does the same, but includes security features to block unauthorized traffic to achieve HIPAA compliance. A firewall can also filter Internet traffic to prevent viruses and other malware from reaching your computers (another HIPAA compliance requirement.) You need a business-grade firewall including the additional subscription-based features to properly protect your network. Recently a $ 400,000 fine was paid when a firewall stopped blocking unauthorized traffic and 17,500 patient records were breached. You can probably figure out that a firewall costs a lot less than the fine and the cost to notify the patients.

RansomWare
RansomWare is malicious software that silently encrypts your data, and then sends a message demanding a ransom payment to get the keys required to unencrypt the files. The cause is often getting a computer user to click on an infected link in an e-mail, or by downloading an infected document.

Ransomware has dramatically increased and ransom fees have increased from a few hundred dollars to thousands of dollars. The unexpected encryption of data has caused a hospital to interrupt patient care and transfer patients to other facilities; costs and business interruptions when data backups were restored instead of a payment for ransom; and delays when organizations had to create BitCoin accounts to pay the fines.

Recently the Office for Civil Rights (OCR) issued guidance stating that a ransomware attack is considered a data breach. While a breach is most often the unauthorized release of PHI, the OCR states that the unauthorized control of PHI, or causing PHI to be unavailable for patient care and other uses, are also breaches.

While a risk assessment may be used to determine if the breach is reportable, requiring patient notification and government reporting, without solid proof that the data has not been removed from the network, a ransomware attack is now considered a reportable data breach.

Cloud Services
Many HIPAA Covered Entities and Business Associates have moved many of their business processes to cloud services, available through the Internet. These range from doctors' Electronic Health Record (EHR) systems; file sharing services; online backups; e-mail, calendars, and contacts; and data storage.

Many cloud services and data centers have denied their obligations by claiming they are not HIPAA Business Associates because:

a. They have no access to their customer's electronic Protected Health Information (ePHI),
b. Their customer's ePHI is encrypted and they don't have the encryption key,

c. They never look at their customer's ePHI,
d. Their customers manage the access to their own ePHI in the cloud,
e. Their terms and conditions prohibit the storage of ePHI, and
f. They only store ePHI 'temporarily' and therefore must be exempt as a 'conduit.'

Each of these excuses has been debunked in HIPAA Cloud Guidance released on October 7, 2016, by the Office for Civil Rights.

The new guidance clearly explains that any cloud vendor that stores ePHI must:

a. Sign a HIPAA Business Associate Agreement,
b. Conduct a HIPAA Security Risk Analysis,
c. Comply with the HIPAA Privacy Rule,
d. Implement HIPAA Security Rule safeguards the ePHI to ensure its confidentiality, integrity, and availability.
e. Comply with the HIPAA Breach Reporting Rule by reporting any breaches of ePHI to its customers, and be directly liable for breaches it has caused.

Professional IT Staff or IT Managed Services

While it may seem like fun for a doctor to manage your network in his spare time, or a good role for his nephew, brother-in-law, or neighbor who can set up a home network, HIPAA compliance requires either a full-time certified staff or a Managed Services arrangement with a professional IT service provider. Managed Service Providers (MSPs) offer remote services that continually monitor and maintain your network at a fraction of the cost of a full-time IT staff.

First, networks that meet HIPAA compliance need to be configured with Security at multiple levels in mind (firewall, PC's, laptops, tablets, smart phones, and servers.) Then they must be monitored and managed to ensure that Security is still working. IT Managed Service providers use remote monitoring and management tools to continually monitor your network, identify problems before they can result in damage, and keep everything updated with security patches. When the $ 400,000 was assessed for the firewall that stopped blocking unauthorized traffic, the HIPAA enforcers noted that the problem was not detected for over 10 months and that proper system activity reviews would have alerted the medical practice much sooner. A Managed Services provider would have likely been alerted immediately. Make sure any outsourced provider signs a Business Associate Agreement and implements a HIPAA compliance program. Managed Services = HIPAA Compliance.

Independent Assessment

For over 12 years we have proven to clients that their self-assessed risk analyses, and beliefs that they had met the requirements for their compliance requirements, that they had missed multiple critical items that could have resulted in a data breach or compliance violation. Our findings prevented issues that had cost others millions of dollars.

Q. Why is it better to have an independent consultant assess your risks and compliance, instead of doing it yourself?

A. Our experience is that while you may be good at running a medical practice, clinic, business, or IT vendor, trying to interpret HIPAA requirements and even using do-it-yourself guidance misses critical items that can easily result in data breaches.

Q. Why is it better to have an independent consultant assess your risks and compliance, instead of using your IT department or outsourced IT vendor?

A. Our experience is that while IT departments and vendors understand networks, an independent consult better understands HIPAA technology guidance and what issues have resulted in financial penalties. Also, an independent consultant is *independent*, and has no bias when looking for issues with compliance and security.

Q. Why is it better to have Semel Consulting assess your risks and compliance, instead of anyone else?

A. Our clients tell us all the time that we discovered risks that they, and others, had missed, and our findings helped protect them against costly and embarrassing data breaches. We are known throughout the healthcare and IT industries as HIPAA and compliance thought leaders. Our founder and lead consultant has spoken to the NASA Occupational Health Conference at the Kennedy Space Center, at the New York State Cyber Security Conference, and numerous IT and healthcare conferences. We regularly have our guidance articles published on healthcare and IT websites. We are the experts who can protect you.

Mike Semel is certified in HIPAA and has been an IT Managed Service Provider, CIO for a hospital, CIO for a K-12 school district, and Chief Operating Officer for a cloud backup company. Mike wrote the Certified HIPAA Security Professional course for 4MedApproved, and helped RapidFire Tools develop its HIPAA module. Mike is certified in Business Continuity planning and helped develop the CompTIA Security Trustmark. Semel Consulting offers a managed compliance services, compliance audits, Meaningful Use Security Risk Analyses, and.business continuity planning.
Visit http://www.semelconsulting.com for more information.