ENJOY SAFER TECHNOLOGY®

HIPAA COMPLIANCE: FOUR ESSENTIAL STEPS

www.eset.com

HIPAA Compliance: Four essential steps

By Michael Aguilar

HIPAA (Health Insurance Portability and Accountability Act) compliance is one of those things that must be done, similar to tying one's shoelaces. You could avoid it and likely get from point A to point B, but one trip on a dangling lace is all it takes to lead to a catastrophe.

For all healthcare organizations, understanding HIPAA compliance will be critical for 2016, especially as the Office for Civil Rights (OCR) begins to conduct the next round of HIPAA audits. Every single healthcare company in the U.S. needs to be prepared for a potential investigation into its data security practices and *approach to HIPAA risk assessments*.

The best practices, controls, and recommendations that are part of becoming compliant all play a vital role in the security of ePHI (electronic protected health information), which includes items such as Social Security numbers, fingerprints, names, and other identifiable information. Failure to secure these items and the facility that houses them could be catastrophic for the healthcare provider or business, including its IT staff and any third-party vendors that have a role within the provider or business's technical infrastructure. So let's go over four important ways to better protect your organization for HIPAA compliance.

1. Planning

Start with a plan. Planning is key and having a good road map will be of great value when undertaking the task of HIPAA compliance. So will the addition of a HIPAA compliance officer to help with the primary planning and deployment of controls—administrative, technical, and physical—to mitigate risk of exposure. To begin, a risk analysis of the organization should be completed to determine shortcomings in the existing security infrastructure (if there is one). This allows assets of the business (such as patient records and billing information) to be ranked in terms of exposure factor and importance. Once the analysis is completed, you'll need to get management on board with your security plan because if there is a breach, they can be held accountable with either criminal or monetary penalties. This includes the in-house IT staff as well as third-party vendors. The fines are based on the level of negligence, and can range from $100 to $50,000 per violation, or per record.

According to a Ponemon Institute study, the average cost of a data breach to a healthcare organization, including fines, monitoring, restitution, etc., is $2.1 million.[1]

Add to that the fact that nearly 40% of consumers say they would stop using a healthcare provider that had been hacked, and the need for compliance is clear.[2]

[1] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2015
[2] Top Health Industry Issues of 2016, PwC Health Research Institute Annual Report, Dec. 2015

2. Administrative Controls

A good place to start is with staff training. As they're the people who will be conducting the business operations day to day, proper training regarding your new security policy will greatly reduce the risk of exposure. Make sure training is an ongoing process, as there are always new threats and means of attack to address. After training, having each individual sign off and acknowledge understanding of the training is crucial.

Statistics back this up. Fully 70% of healthcare organizations cited employee negligence as their biggest security threat.[3] Items that the staff policy and procedure should cover are basics: how to access your machine, what to do and what not to do online, how to ensure data security by not leaving devices unlocked, and other items that may seem obvious but could be completely missed by someone not familiar with HIPAA compliance. After the staff is trained, you can start placing technical controls to reduce the risk of breach or exposure.

3. Technical Controls

There are many ways to ensure the safety of your organization by placing the correct controls in place. Some of these controls are pretty basic, such as the need for endpoint protection software to ensure that machines

[3] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data

Product features aligned for compliance issues

	CIPA	FERPA	GLBA	HIPAA	PCI	SOX	HITECH
Antivirus/ Anti-Malware	⚪	⚪	🔵	🔵	🔵	🔵	
Personal Firewall			⚪	⚪	⚪		
Encryption		⚪	🔵	🔵	🔵	🔵	
Two-Factor Authentication		⚪	🔵	🔴	🔵	🔴	🔴
Central Management					🔵		

🔵 Required 🔴 Recommended, not required ⚪ Not required nor recommended

are not compromised. While any kind of endpoint protection is an improvement over none at all, paid versions are generally far better than “freemium” versions due to functionality of the full suite of software and other aspects that may be turned off on free versions. And, you need to keep in mind that simply installing Internet security software doesn’t make you HIPAA compliant. Compliance is an ongoing process, not a checkbox, and you need a multilayered security approach to maintain it.

ESET Endpoint Security can help mitigate the risk of users going to non-work-related sites through the use of the Web Control module which can block access, allow only certain user groups to access open Internet, or other variations depending on user needs. You can also enable items such as ESET Anti-Phishing protection at the client level to reduce risk of receiving spam and infected emails.

ESET endpoint builds will provide antivirus, antimalware, and protection against malicious parties that may be trying to access your data. For instance, if somehow a rogue machine on the network was able to perform a MITM (man in the middle) attack, the ESET Personal Firewall on the computer would alert the operator and block the traffic from being redirected to the rogue machine’s spoofed MAC address.

Phones are also not immune to being targeted. With a recent survey [4] showing that nearly 90% of healthcare organizations use at least one type of mobile device to engage patients, and that 57% have enabled text communications, mobile security must be part of your plan.

Products like **ESET Mobile Security for Android** can help reduce the risk of exposure by limiting application usage, ensuring password complexity, removing malicious packages, and providing anti-theft features that can help to recover or remotely wipe a device if it is lost. This becomes especially useful with the prevalence of BYOD in the workplace—allowing some security control of the device, while still retaining the usability from an end-user perspective.

Two other important ways to enhance the security of data transmission and integrity, and availability of your ePHI, are encryption and backups.

Encryption software such as **DESlock+ Enterprise** enables users to send encrypted files between parties, allowing only specified users to be able to access them. Access to files is granted through a key exchange that can be set up from the DESlock+ Enterprise Server, removing the end users from the equation. The encryption ciphers used (RSA 1024, AES-128/256, SHA256/160, Triple DES 112, and Blowfish 128) are nearly unbreakable and if somehow an unauthorized party were to gain access to the encrypted drive, the files would be useless. DESlock+ solutions are also FIPS 140-2 level 1 certified.

You also need to plan for the worst scenario. If your entire site goes down due to a disaster, technical failure, weather, or other issue—such as a ransomware attack—you will thank every person you know if you have a good backup solution in place.

If you don't, you may be facing a situation like the one at Hollywood Presbyterian Medical Center, where computers were locked up for nearly two weeks after being infected by ransomware on February 5. The hospital couldn't access patient medical records, test results, or emails until they paid the attackers about $17,000—a situation that could have been avoided if their data had been regularly backed up.

StorageCraft offers multiple products to back up, manage backups, replicate, and assist if your site needs to recover from a disaster. Its offerings include workstation recovery via ShadowProtect Desktop, server recovery with ShadowProtect Server, and ShadowProtect Virtual to restore virtual machines. The company even has standalone tools to recover lost emails in a Microsoft Exchange environment. And if the entire site is offline, files can be accessed by remote users with an Internet connection.

[4] The State of Cybersecurity in Healthcare Organizations in 2016, Ponemon Institute, Feb. 2016

4. Physical Security

Obviously, you will need to ensure that areas like server rooms and critical infrastructure are protected from access by unauthorized parties, by using either physical or electronic locking systems such as key-card badges. Mantraps also help by ensuring the party entering the protected area is either verified by security or videotaped while accessing the protected asset. Although I have not seen them in use for some time, physical key-based locking systems are not recommended as they are easily bypassed. Even the heartiest padlock can be picked if the user is persistent enough.

Summary

HIPAA compliance and planning is a major undertaking. Once completed, it does not stop as you need to re-assess your security posture, re-analyze your weak points, and possibly tweak a few controls to get things right where you need them to be. Having a powerful, multilayered security solution that protects systems, users, and data throughout your organization will help mitigate a lot of the risk, as will keeping employees up to date on training.

If you are just starting this process for the first time, *www.HealthIT.gov* has a free security assessment tool to help you begin planning. It will visually help you to gather the required info to create a roadmap of what you need—and successfully complete the project.

Learn more. Read *The State of Cybersecurity in Healthcare Organizations in 2016* report.

Michael Aguilar is a business product technical lead at ESET North America. He is studying for the CISSP exam and has a Security+ certification as well as a Usable Security certification from the University of Maryland Cyber Security Center via Coursera.org. He is currently responsible for working with large-scale clients for ESET North America and works with ESET developers, QA, and support engineers to resolve issues with clients in a quick and effective manner. Michael is active on Spiceworks and various security forums looking at new threat vectors and the best controls to mitigate those risks.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit ***www.eset.com****.*

ENJOY SAFER TECHNOLOGY®