"A review of Data Encryption of Protected Healthcare Information as it relates to HIPAA and HITECH compliance."

Mike Richter

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 laid the framework for the privacy and security of Protected Health Information (PHI). The original law focused on three main provisions, "(1) the portability provisions, (2) the tax provisions, and (3) the administrative simplification provision" (Nass SJ, 2009) It is the third provisions which covered electronic medical record and the need to secure the data and maintain the privacy of the patients. According to Nass, "The primary purpose of these provisions was to standardize the use of electronic health information, but Congress also recognized that advances in electronic technology could endanger the privacy of health information" (Nass SJ, 2009). It was this fear that lead to provisions that would become known as the Security Rule. According to the Department of Health and Human Services website, "The HIPAA Security Rule establishes national standards to protect individuals electronic personal health information that is created, received, used, or maintained by a covered entity" (hhs.gov, 2014) The purpose of this paper is to look at how different types of data encryption can be used to enforce the standards found in the original HIPAA law as well as the laws that came after it, HITECH and the HIPAA omnibus final rule of 2013.

The text of the Security Rule itself defines encryption the following way, "Encryption Refers to transforming confidential plaintext into cipher text to protect it. An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes intelligible." (Security and Electronic Signature Standards 45 CFR Part 142, 1998) While the rule does define Encryption it does not require it. The 1998 law defines Access Control as a

requirement by stating, “The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based Access. The use of Encryption is optional.” (Security and Electronic Signature Standards 45 CFR Part 142, 1998) Encryption is seen as a method to achieve these goals but not a goal in itself. While the law does not categorize encryption as required it does categorize it as addressable. Reber states on encryption that, “It will not necessarily reduce your risk of a privacy breach nor will it protect you from HIPAA violations. Encryption is broken with a password.” (Reber, 2011) Without proper security controls and policies, encryption alone cannot protect PHI. However it can a crucial tool in HIPAA compliance. The HSS website states that encryption is “addressable, and must therefore be implemented if, after a risk assessment, the entity has determined that the specifications is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI.” (hhs.gov, 2014) Given the complexity and availability of current Electronic Medical Record Systems, it would be difficult to not choose to encrypt data, the question is: when, where, and what encryption techniques should be used to maintain compliance with these rules.

It is clear that encryption is a vital tool in maintain privacy and security of Electronic Protected Health Information (ePHI). However where and how it is to be used is open to debate. There two primary states where data can be encrypted, in-transit across data networks, and at rest on user devices. We will first look at encryption at rest on data at rest. The most vulnerable location for sensitive data is on a user’s device. These devices, whether they be a desktop, laptop, or mobile devices, are the most likely to be stolen or misplaced and expose sensitive data to attack. According to the HIPAA Breach Notification Rule (45 CFR §§ 164.400-414) , if a

device is stolen or misplaced, a covered entity is required to report the loss of ePHI to regulators and to the individuals involved in the breach. The law does allow for an exception in the form of the "Safe Harbor" provision. This states that "if the covered entity of business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information" (HSS.gov, 2014) The primary way to accomplish this provision is to provide proof of strong encryption of the endpoint device. To qualify for this, adequate encryption practices and key management must be maintained. We will look at the three methods defined by NIST in Special Publication 800-111, "Guide to Storage Encryption Technology for End User Devices". These methods are Full Disk Encryption, Virtual Disk and Volume Encryption, and File/Folder Encryptions".

NIST defines Full Disk Encryption (FDE) as, "The process of encrypting all the data on the hard drive used to boot a computer's OS, and permitting access to the data only after successful authentication to the FDE product." (Scarfone, Souppaya, & Sexton, 2007). This method will encrypts the entire drive as well as the boot sector for the drive. A separate Preboot OS is installed to provide authentication into the encrypted boot sector and standard OS. Once in the OS, files are encrypted and decrypted on demand as needed. This cause some performance delays. According to NIST, "This may marginally increase the time needed to open or save files, but the delay generally should only be noticeable for particularly large files." (Scarfone, Souppaya, & Sexton, 2007) . Key management an important piece of a FDE strategy. It is what "enables you to revoke and manage keys in any way". (Brandel, 2009) If used with a centralized Key Management system, FDE provides strong assurances that sensitive data will be protected a device is misplaced or stolen. NIST states "For a computer that is not booted, all the information encrypted by FDE is protected, assuming that pre-boot authentication is required."

(Scarfone, Souppaya, & Sexton, 2007) However, the flaw in FDE is that once a device is booted and authenticated, full access to files is available. This could be problematic for Safe Harbor provisions if the state of the device when misplaced or stolen is not known. FDE is most effective with traditional computing devices such as laptops or desktops.

While FDE provides significant assurance that data on an end user device is protected, it is not always the most appropriate method of encrypting data. Virtual Disk encryption is a "the process of encrypting a file called a container, which can hold many files and folders , and permitting access to the data within the container only after proper authentication is provided, at which point the container is typically mounted as a virtual disk." (Scarfone, Souppaya, & Sexton, 2007) Unlike FDE, this allows unencrypted and encrypted data to exist simultaneously on the same device. When the end user needs to encrypt a file they copy it to the container. "The data is encrypted dynamically and stored on the disk by virtual disk encryption driver." (Chang, Liang, & Kou, 2010). The user does not need to manually perform a decryption process to read the data. "When the data is read from the virtual disk partition, it is decrypted by virtual disk encryption driver and is in plaintext to the user." (Chang, Liang, & Kou, 2010) This on demand encryption does not have the same performance issues as FDE, but it requires the user to be knowledgeable of what needs to be encrypted.

A similar use of this technology is Volume Encryption. Instead of encrypting a portion of the disk as a container, Volume encryption "is the process of encrypting an entire logical volume and permitting access to the data on the volume only after proper authentication is provided." (Scarfone, Souppaya, & Sexton, 2007) This technology is often used for portable media such as USB drives and portable hard drives. This allows data to be carried to be transported on portable storage without the risk of data being compromised by misplacing the

drive or having the drive stolen. While the technology is similar, there are differences between Virtual Disk and Volume Encryption. "The key difference between volume and virtual disk encryption is that containers are portable and volume are not- a container can be copied from one medium to another, with encryption intact." (Scarfone, Souppaya, & Sexton, 2007) This is an advantage in managing encrypted data as it moves locations within a computer system.

Virtual Disk and Volume Encryption can be useful tools when seeking to utilize the "Safe Harbor" Provision. For example, if a USB drive encrypted with Volume Encryption goes missing, it would qualify for the "Safe Harbor" provision. As with FDE documentation, central management, and strong key management are crucial to applying this provision successfully. For instance it must be shown that you have followed standard key management provisions such as not storing the public and private keys with the data. Additionally, Virtual Disk Encryption, like FDE, is only effective if the machine is not logged in. If logged in and "single-sign is being used for authentication to the solutions, this usually means the containers are protected until the user logs onto the device. If single sign-on is not being used, then protection is typically provided until the user explicitly authenticates to the container.". (Scarfone, Souppaya, & Sexton, 2007) This shows the difficulty in balancing user convenience and information security. To best secure date in a Virtual Disk Encryption scenario, it is best to force them to authenticate when accessing an encrypted portion of the file system. However, from a usability standpoint, a single sign on solution is highly preferable. In a PHI scenario, it would be best to forgo the single sign-on since it would increase the difficulty of applying the Safe Harbor provisions should the device go missing.

The final endpoint encryption technology that we will investigate is File/Folder encryption. "File encryption is the process of encrypting individual files on a storage medium

and permitting access to the encrypted data only after proper authentication is provided. Folder encryption is very similar to file encryption, only it addresses individual folders instead of files." (Scarfone, Souppaya, & Sexton, 2007) This type of encryption has similar functionally as Virtual Disk and Volume encryption, but the mechanics differ. In the Virtual Disk encryptions, " A container is a single opaque file, meaning that no one can see what files or folders are inside the container until the container is decrypted. File/folder encryption is transparent, meaning that anyone with access to the filesystem can view the names and possibly other metadata for the encrypted files and folders." (Scarfone, Souppaya, & Sexton, 2007) Like Virtual Disk and Volume encryption, File/Folder encryption is vulnerable if used in a single sign-on setup. Additionally since file names and other metadata is accessible without authentications, it is possible for an attacker to gain valuable information from this data without actually accessing the encrypted data. Due to these limitations, this type of encryption is the least effective when attempting to qualify for the "Safe Harbor" provisions.

Data at-rest on endpoint devices is amongst the most vulnerable states for PHI. As devices and data storage gets smaller and more portable, it is important to use strong encryption techniques to guard against data breaches. With data at rest, it is easier to determent when a breach occurs. When a device goes missing, it can be determined whether that data was encrypted or not and if a breach of PHI has occurred and needs to be reported. With data in transit on a network, if proper encryption and intrusion detection techniques are not used, it is easier for attackers to obtain sensitive PHI without being detected. We will look at encryption techniques that will satisfy the HIPPA requirements on both internal and external networks, as well as wireless networks that increasingly carry highly sensitive health data.

With the passage of the HITECH legislation of 2009, healthcare providers were compelled to move medical records into Electronic Medical Record (EMR) systems. These are large, complex systems that transfer sensitive ePHI across private and public networks. This ePHI in transit is vulnerable to a variety of attacks including packet sniffing and man-in-the-middle attacks. To guard against this, it is vital to use strong encryption standards when this information is transferred outside the secured internal network. Once method is to use a suite of secure protocols such as IPSEC. "Internet Protocol Security (IPSec) is a suite of network layer security protocols frequently used to establish virtual private networks." (Stine & Dang, 2011) This virtual private network assures that only the two end devices can understand the message and any party in the middle will only see undecipherable cipher text. IPsec is applicable to a variety of network traffic, but often requires specialized setup and configuration on both sides of the connection. The more specific protocols of SSL and TLS are focused primarily on web traffic and are available through most modern web browsers. With "Secure Socket Layer (SSL) or Transport Layer Security(TLS) protocols, the use of encryption may be transparent to users." (Stine & Dang, 2011) This user transparency is advantageous in a fast-paced healthcare environment. Using strong encryption to protect ePHI is important to maintaining HIPAA compliance, but simply setting up encryption protocols will not necessarily maintain the level of security and privacy needed. The longer an encryption technique is in common use, the more likely it is to become susceptible to attacks. SSL, mentioned above, was once considered the gold standard of network encryption techniques. Recently, researchers at Google showed that SSL's "POODLE (Padding Oracle On Downgraded Legacy Encryption) exploit allows blackhats to steal secure cookies or bearer tokens" (Hruska, 2014) Now if a healthcare organization is using SSL 3.0 "it's relatively simple for an attacker with man-in-the-middle access between

client and server to decrypt cookies and access secure information." (Hruska, 2014) The need to stay up to date on encryption techniques and their vulnerabilities is almost as important as encryption itself when it comes to maintain HIPAA compliance and avoiding a data breach.

It is vital to used strong encryption techniques when sending ePHI across public networks, however even within secured networks protected by a strong firewall and intrusion detection techniques it is also important to maintain a strong level of encryption to protect ePHI. While internal networks are seen as more secure, it is important to recognize that data in transit needs to be secured as effectively as on external networks. Strong encryptions such as TLS should be used when available for internal communications. Additionally, since internal networks are more controlled environments easier to maintain strong key management standards that help ensure the security of the encrypted data.

One area of concern within internal networks is wireless communications. In the healthcare setting, it is not only traditional application level ePHI sent through the air on wireless signals, it is also raw clinical data sent from medical devices. This data is of the highest sensitivity since tampering with it could cause harm or even death to a patient. This is a point where the vagueness in HIPAA is problematic as it comes to patient safety. According to Baker, Knudsen , and Ahmaidi, HIPAA only suggests encryptions and even then doesn't specify the strength. This may cause organizations to go with the cheapest and simplest forms of encryptions. "Unfortunately, the simple encryptions available in the cheapest wireless solutions is not enough to safeguard medical devices, patient data, and the enterprise network. Wired Equivalent Privacy (WEP) and preshared keys (PSK) used in Wi-Fi Protected Access (WPS/WPA2) can be compromised in a matter of seconds!" (Baker, Jonathan, & Ahmadi, 2013) While HIPAA and HITECH do not specify specific encryption techniques, they do maintain that

all efforts to prevent data breach much be made. The current standard is WPA2-enterprise with AES. WEP and WPA are no longer seen as secure standards. WEP encryption was broken years ago and "WPA was developed as an interim solution until hardware support for WPA2 and AES was available. It was never intended to be the long-term security solution and should be avoided as should WEP." (Baker, Jonathan, & Ahmadi, 2013) This again shows the need to stay up to date on encryption technologies to maintain HIPAA compliance. While the law does not specify the use of encryption techniques, if data is leaked due a WEP encryption on a consumer grade access point it still considered a data breach even with encryptions being deployed.

While traditional wireless access provides a security and encryption challenge, increasingly personal mobile phones and tablets are being used to access ePHI. Healthit.gov provides several recommendations for encryption on mobile devices. To meet federal regulations, they suggest "Encrypting the data on your mobile device with a valid encryption process consistent with FIPS 140-2" (Healthit.gov, 2014). Additionally, they caution against using text messaging using Short Message Service (SMS) for PHI since this will send the data unencrypted. They suggest "consider using secure messaging which is encrypted instead of SMS which is not" (Healthit.gov, 2014) Finally they recommend encrypting data in motion using " a virtual private network (VPN) or a secure browser connection"." (Healthit.gov, 2014) These suggestions are similar to suggestions above for end user devices, but the difficulty is increased since mobile devices are often not owned or managed by the organization. Recently, organizations have begun to require end users who access ePHI to subscribe to the organizations Mobile Device Management (MDM) platform. This allows the organization to enforce encryption rules for ePHI on these personal devices. This give the healthcare organization the

ability maintain the security and privacy of patient information in accordance with HIPAA and HITECH.

The HIPAA and HITECH legislation require safeguarding the privacy and security of patient information. In recent years there has been a move to transfer this information from paper records to electronic records. This transition has led to significant challenges within Information Security. While a useful tool for protecting ePHI, encryption alone does not guarantee HIPAA compliance. It can only be effective with proper planning, key management, access control policies and consistent upkeep and maintenance. Additionally it must be utilized in all states of data, at-rest and in-motion, internal and external, fixed and mobile. If used effectively, Encryption can help achieve the security rule's goal of establishing a "national standards to protect individuals electronic personal health information that is created, received, used, or maintained by a covered entity" (hhs.gov, 2014)

References

Baker, S., Jonathan, K., & Ahmadi, M. (2013). The Wireless Challenge: Security and Safety For Medical Devices and Hospitals. *Biomedical Instrumentation and Technology*, 208-11.

Brandel, M. (2009, 10 21). *Full Disk Encryption Dos and Don'ts.* Retrieved from www.csoonline.com: http://www.csoonline.com/article/2124486/data-protection/full-disk-encryption-dos-and-don-ts.html

Chang, C., Liang, M., & Kou, H. (2010). A Review of Encryption Storage. *Information Technology Journal*, 1517-1520.

Healthit.gov. (2014, 11 23). Retrieved from healthit.gov: http://www.healthit.gov/providers-professionals/2-install-and-enable-encryption

hhs.gov. (2014). Retrieved 11 11, 2014, from http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2001.html

hhs.gov. (2014). Retrieved 11 11, 2014, from www.hhs.gov: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

Hruska, J. (2014, October 15). Google finds critical vulnerability in SSL called POODLE. *ExtremeTech.com*.

HSS.gov. (2014, 11 16). Retrieved from www.hhs.gov: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

Nass SJ, L. L. (2009). *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research.* Washington, DC: National Acadamies Press (US).

Reber, E. (2011). Five Steps to Achieving HIPAA Compliance. *Biomedical Instrumentation and Technology , 45*(5), 360-3.

Scarfone, K., Souppaya, M., & Sexton, M. (2007). *Recommendations of the National Institute of Standards and Technology.* Gaithersburg, MD: National Institute of Standards and Technology.

Security and Electronic Signature Standards 45 CFR Part 142 (1998).

Stine, K., & Dang, Q. (2011). Encryption Basics. *Journal of AHIMA*, 44-46.