Risk Assessment Toolkit

Addressing Encryption of Data at Rest in the HIPAA Security Rule and EHR Incentive Program Stage 2 Core Measures

Introduction

Recent analysis of the Department of Health and Human Services (HHS) reported breach data indicates that a significant percentage of large breaches involve lost or stolen laptops and other portable devices.[1] Had the data stored on these devices been properly encrypted, the data would have been secure; breach notification by the covered entity would not have been required; and the individuals whose data was breached would not have been subject to the risk of identity theft and fraud, or the stress of receiving a breach notice. This illustrates why the HIPAA Security Rule of 2003 includes an addressable implementation specification for encryption of data at rest and why one of the EHR Incentive Program Stage 2 core measures requires that encryption of data at rest be addressed in a risk assessment of the certified EHR.

Purpose of this Paper

The purpose of this paper is to help healthcare providers understand the HIPAA requirement for encryption of data at rest and apply it appropriately to their IT environments. The HIMSS Privacy and Security Risk Assessment Working Group developed this paper to give an introduction to encryption and explain how a physician practice, hospital or any HIPAA covered entity or business associate should evaluate what electronic protected health information (ePHI) to encrypt. We will outline and illustrate the process to conduct this evaluation. We will also provide guidance to understand the different types of encryption and encryption tools.

Background on EHR Incentive Program

In the Centers for Medicare and Medicaid Services' (CMS) EHR Incentive Program, the Stage 1 Meaningful Use Core Measures include a measure mapped to the objective to "protect electronic health information created or maintained by the certified EHR technology". The Stage 1 measure for that objective is to "conduct or review a security risk analysis…"[2]

---

[1] U.S. Department of Health & Human Services. Breaches Affecting 500 or More Individuals. [website]. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[2] 42 FR 412, 413, 422 et al (2010-07-28). Available at: http://www.gpo.gov/fdsys/pkg/FR-2010-07-28/pdf/2010-17207.pdf

On August 23, 2012, the CMS released the final rule for the Stage 2 measures. The Stage 2 core measures have a nearly identical requirement for a security risk analysis. But the Stage 2 core measure expands on the requirement placing added emphasis on encryption. The Stage 2 core measure for a security risk analysis in its entirety states:

> Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data stored in CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process[3] (Emphasis added)

We should keep in mind that this requirement is simply restating and reinforcing the encryption requirement found in the HIPAA Security Rule under the standard for access control (45 CFR 164.312(a)(2)(iv)). What this means is that a longstanding, but possibly unclear, requirement to encrypt data at rest is now receiving a great deal of well-deserved attention.

Encryption

An in-depth explanation of encryption is beyond the scope of this paper.[4] Simply put, encryption is a technique to prevent access to sensitive data by replacing the sensitive plain text data with illegible cipher text. The plain text is altered by a computer program to make it unreadable, creating the cipher text. Only the cipher text is stored on the computer. Decryption is the technique of using a computer program to reconstruct the plain text from the cipher text.

Encryption depends on sophisticated mathematical algorithms. Some common encryption algorithms used for data at rest have names like AES, DES, Triple DES, SKIPJACK, Blowfish and Twofish. These encryption algorithms are not secret. The algorithms make use of the plain text and a secret key to create the cipher text. The same secret key and cipher text are used to recreate the plain text. This type of encryption is called symmetric encryption.

Another type of encryption, called asymmetric encryption, uses a public-private key pair. The plain text is encrypted with a public key by the sender. The recipient decrypts the cipher text data with a private key to which only the recipient has access. Thus, the receiving party is the only one capable of decrypting and reading the encrypted messages.

The best encryption programs make it nearly impossible (or at least prohibitively expensive) to re-create the plain text from the cipher text without the secret key. The secret key is typically stored on the computer

[3] 42 FR 170 (2012-09-04). Available at: http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf

[4] For a more in-depth description of encryption see NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook especially chapter 19 on Cryptography as well as section 17.3.1.2 on encryption. Note, this publication was published in October 1995, and some information is out of date. For example, it states that DES provides an acceptable level of encryption. This is no longer true. For a more up to date description of encryption of data at rest see NIST Special Publication 800-111 *Guide to Storage Encryption Technologies for End User Devices, November 2007*

hard drive, along with the data, but is protected by password. It is important to select a strong password[5] and protect the password from unauthorized disclosure[6].

Not all encryption is equally strong. In 2000, the National Institute of Standards and Technology (NIST) sponsored a competition to identify the best available encryption algorithm. The Rijndael algorithm won the competition and has been designated the current advanced encryption standard (AES).[7] [8]

In response to the requirement of the HITECH act of 2009, HHS published the *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements*…, 45 CFR Parts 160 and 164 (April 27, 2009)[9]. This federal law states that the NIST Special Publication 800-111 *Guide to Storage Encryption Technologies for End User Devices* is the authoritative standard for an acceptable level of encryption for data at rest. The Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules* is another authoritative resource for determining adequate levels of encryption. Note that standards for adequate encryption levels change periodically due to ever-increasing computer processing power and continuous advances in hacking techniques.

AES encryption with a key strength of at least 128 bits is a minimum level of encryption for protecting ePHI data at rest. [10]

Considerations for Encryption of Data on Various Storage Media

One of the technical safeguard standards of the HIPAA Security Rule is access control, which requires a covered entity to "implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights…."[11] One method to control access to ePHI is to encrypt the data. Indeed, one of the HIPAA Security Rule implementation specifications of this particular safeguard is exactly that—to "implement a mechanism to encrypt and decrypt electronic protected health information."

Data at rest refers to data wherever it is stored. A provider's EHR software or practice management systems are not the only places where ePHI may be stored. Examples of devices and media which may store ePHI include computer disk drives (server, workstation, laptop, etc.), USB flash drives, flash cards, CDs, DVDs, back-up tapes, tablets, smartphones, copy machines, digital voice recorders and electronic medical devices. As such, all of these devices and media must be considered as part of an overall HIPAA

[5] NIST SP 800-118. Password strength is determined by a password's length and its complexity, which is determined by the unpredictability of its characters.

[6] NIST SP 800-118. Guide to Enterprise Password Management (Draft). This document provides a good reference for organizations to develop good password management policies.

[7] American Medical Association. HIPAA security rule: frequently asked questions regarding encryption of personal health information. 2010. Avilable at: http://www.ama-assn.org/resources/doc/psa/hipaa-phi-encryption.pdf. Accessed August 12, 2012.

[8] National Institute of Standards and Technology. Commerce department announces winner of global information security competition. October 2, 2000. Available at: http://www.nist.gov/public_affairs/releases/g00-176.cfm. Accessed August 12, 2012.

[9] 74 FR 79. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf.

[10] NIST Special Publication 800-131A. Transitions: recommendation for transitioning the use of cryptographic algorithms and key lengths. January 2011. Table 1 (3-4).

[11] HIPAA Security Rule, §164.312. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf

Security Rule compliance program, including evaluating and implementing encryption capabilities or alternatives in your organization.

Each type of device or media will have unique considerations for how to encrypt the data stored on the storage media. For example, many copy machine manufacturers offer an optional encryption module that must be purchased separately. Some smartphones have encryption capabilities included, but they must be configured to enable it. Other smartphones may require an additional component or third-party product to enable encryption. This paper cannot describe specifically how to encrypt data for each type of device. For more information about encrypting the data for specific media you may need to contact the manufacturer or re-seller of your devices.

Types of Encryption

The NIST *Special Publication 800-111 - Guide to Storage Encryption Technologies for End User Devices* describes the following types of encryption technologies:

- Full-disk encryption (FDE).
- Virtual disk encryption and volume disk encryption.
- File/folder encryption.

Full-Disk Encryption

Full-disk (or whole disk) encryption is the process of encrypting all the data and files (including system files) on the hard disk. Full-disk encryption software is most commonly used on desktop and laptop computers.

Virtual Disk and Volume Encryption

Virtual disk encryption is the process of encrypting a file called a container, which holds many files and folders. Access to the data within the container is provided only after proper authentication.

Volume encryption is the process of encrypting an entire logical volume and permitting access to the data after appropriate authentication. Volume encryption is suited for hard drive data volumes and volume-based removable media, such as USB flash drives and external hard drives.

File and Folder Encryption

File encryption is the process of encrypting individual files on a storage medium and permitting access only after appropriate authentication. Folder encryption is similar to file encryption, whereas it encrypts individual folders instead of files. File/folder encryption allows anyone with access to the file system to view the names and possibly other information for the encrypted files and folders. File/folder encryption is used on all types of storage for end-user devices.

Encryption Tools

There are numerous tools that provide encryption. Some must be purchased, but there are some free and low-cost options.

Microsoft Encrypting File System (MS EFS)

MS EFS is a feature of Microsoft Windows that can be used to store hard disk information in an encrypted format. More information is available here.

Windows 7 Bit Locker Drive Encryption
Bit Locker allows you to encrypt all data stored on the Windows operating system volume and configured data volumes. More information is available here.

Microsoft Office 2007 SP3 and above
MS Office 2007 SP3 and above includes AES encryption. More information is available here.

TrueCrypt
TrueCrypt is an open-source encryption product. Depending on the operating system, it can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device. More information is available here.

Endpoint Security Vendors
Many of the endpoint security vendors who are well known for antivirus software also make excellent encryption products. Contact your antivirus software vendor to see if they make an encryption product that you can license. Be sure to verify that a FIPS 140-2 compliant encryption is used.

Required vs. Addressable Specifications in the HIPAA Security Rule

The encryption of ePHI as described in this paper is an addressable implementation specification rather than a required implementation specification, according to the HIPAA Security Rule. The Security Rule's addressable specifications are not simply optional. If the addressable implementation specification is "reasonable and appropriate" for the covered entity it must be implemented. However, if an addressable implementation specification is not reasonable and appropriate for the covered entity, an equivalent alternative implementation may be adopted if that alternative is reasonable and appropriate and achieves the same purpose. Or, if it is determined that the security standard is otherwise met or that the identified risk is negligible, and such determinations are documented, an addressable implementation may be left not implemented.

When deciding if an addressable implementation specification, its equivalent alternative or a strategy of non-implementation is reasonable and appropriate, a risk analysis should be conducted. The final decision for satisfying an addressable implementation specification should consider a variety of factors, including a current risk analysis, existing security controls, risk mitigation strategies and implementation costs. As part of an overall HIPAA Security Rule compliance program, the factors that constitute this decision-making process, including the results of the risk analysis, must be documented to support the decision. Documentation should be maintained and may be required in the event of a HIPAA compliance audit or may, in the future, need to be submitted for Meaningful Use attestation.

This documentation should be maintained consistently with HIPAA Security Rule documentation requirements.[12] The HIPAA Security Rule's documentation standard includes the following implementation specifications (all of which are required):

- Retention: "Retain the documentation required … for six years from the date of its creation, or the date when it was last in effect, whichever is later."

[12] HIPAA Security Rule, §164.316. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

- Availability: "Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains."
- Updating: "Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of electronic protected health information."

Deciding Whether to Encrypt — An Example

Given that encryption of data at rest is addressable, how does one decide if encryption is "reasonable and appropriate?" To walk through the decision process, let's consider an example.

Scenario: Consider an organization that uses laptops. In this example, the laptops are used by homecare nurses and there is ePHI stored on the laptops.

Threats/Vulnerabilities: Since the laptops are carried by nurses throughout the community in their cars, into patient homes and stored in the nurse's home at the end of the day, the laptops are clearly vulnerable to being lost or stolen.

Likelihood: In the past several years there have been several incidents of laptops being lost or stolen in this organization. It is also observed that in the CMS *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2009 and 2010*[13], theft was the most frequent cause of breaches, followed by loss of device. Of the 99 incidents involving theft, 42 involved laptops. Several of the losses were also laptops[14]. So, the likelihood that laptops will be lost or stolen in the future is not negligible and is probably high given that about 100 nurses and clinicians use and transport laptops daily.

Impact: Next, the type of harm that would occur is evaluated (the impact). Since the laptop hard drives store clinical, demographic and some financial information on all of the patients in the nurse's caseload (up to 200 patients), the level of harm to the organization is considerable. It is noted that recent published estimates regarding the cost of a data breach found the average cost to an organization averaged $204 per record.[15] So for a breach of 200 records the impact to the organization of a single lost or stolen laptop is likely to be over $40,000. In addition, there would be legal and regulatory impacts. The HITECH breach notification requirement requires notification of HHS, in addition to notifying the affected individuals. The notification to the federal government would likely trigger an investigation and possible fines. (There may also be state laws regarding breaches of personally identifiable information (PII) that could trigger investigations and fines.) Clearly the impact of a lost laptop with unencrypted ePHI is high.

Existing Safeguards (Controls): Access controls are used. The laptops are all protected by Microsoft Windows authentication and strong passwords are used. The nurses are careful to log out when they are not using the laptops, and they do not tape the passwords to the laptop. But when evaluating the risk, the IT support analyst explains that the access controls can easily be bypassed. The hard drive can be

[13] U.S. Department of Health & Human Services. Annual report to congress on breaches of unsecured protected health information. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf. Accessed May 15, 2012.

[14] *Ibid*.

[15] *Second Annual Benchmark Study on Patient Privacy & Data Security*, The Ponemon Institute. December 2011.

removed from the laptop and read by another computer without having to login to the Microsoft Windows operating system on the laptop. So the existing safeguards do not provide sufficient protection.

Conclusion

Since the likelihood of a breach of ePHI due to a lost or stolen laptop is high, the harm is high and the existing safeguards are not adequate, there is an overall high risk of a breach of ePHI and patient privacy due to the loss or theft of a laptop. Encryption of the data stored on the laptop hard drive would substantially reduce the likelihood that ePHI could be accessed. Therefore encryption is reasonable and appropriate.

Consideration can be given to the cost of encryption and the level of effort to implement and support encryption, but today the cost of encryption is not high (there are even some free encryption solutions) and encryption has become fairly commonplace. It might take some time, but the existing IT staff can develop and implement an encryption solution, or a consultant could assist. The conclusion is that encryption is a reasonable and appropriate safeguard for the homecare laptops. The organization carefully documents their analysis and makes plans to encrypt the laptops.

This type of risk analysis can be repeated for other types of devices and threat/vulnerability scenarios. Here are some basic considerations:

- Begin by reviewing an inventory of all of the devices and media that are used to store ePHI. For each device or media type evaluate the risks of unauthorized use or disclosure of ePHI.
- There may be many types of devices that are at risk of loss, theft or improper disposal and should be considered as candidates for encryption. A few examples are USB drives, backup tapes, smartphones, desktop PCs, tablets, cameras, biomedical equipment, copiers, fax machines, printers and multifunction devices.
- There may be some types of devices that would never have ePHI stored on them, so encryption may not be reasonable and appropriate.

Compensating Controls (Safeguards)

If the decision is made that encryption is not or may not be a reasonable and appropriate safeguard the organization must document why it is not reasonable and appropriate and then evaluate whether there is some other safeguard which is reasonable and appropriate. In this section we will describe and evaluate some possible compensating controls[16] for encryption of data at rest.

There is no single safeguard that can universally compensate for data encryption. In fact, encryption is such a good safeguard, that it may be hard to decide against encryption as the best safeguard in many scenarios. (The fact that encryption is identified as a safe harbor from the breach notification requirements of the HITECH Act makes it highly desirable for risk mitigation.[17]) The previous example of laptop risks illustrates this well.

---

[16] Note: the term "compensating controls" is commonly used to describe acceptable alternatives to a required control or safeguard.

[17] U.S. Department of Health & Human Services. HITECH Breach Notification Interim Final Rule. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html.

Breach Notification Interim Final Rule: http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf.

In this section we will list some safeguards that may be considered alternatives to encryption. We also will include encryption of data at rest in the list. For each safeguard we will briefly describe the advantages and disadvantages of the safeguard as a compensating control for not encrypting media with ePHI. Note, this list is representative of available alternatives and not a comprehensive list of possible compensating controls for encryption.[18]

Possible Alternatives to Encryption		
Safeguard (Compensating Control)	Advantages/Strengths	Disadvantages/Weaknesses
Physical Controls		
Inventory control/asset tracking.	Can detect if a device is lost or stolen.	Does nothing to prevent a device from being lost or stolen.
Store removable media in locked containers or in secure locations.	Only protects the removable media while it is stored.	Provides no protection when the removable media is in use or is being transported.
Locate servers in locked rooms/data centers.	Prevents or deters theft of servers and server drives	Does not protect the data from hackers and cybercriminals who may breach network security. Does not solve the problem of how to return a drive for warranty repair if it cannot be wiped (data completely removed).
Video surveillance and recording.	Deters theft and may support investigation and recovery after a security incident.	Deters, but does not prevent, theft or unauthorized access.
Attach laptops / desktops to furniture (i.e. with cables or bolts).	Deters theft.	Does not prevent theft, only deters it.
Attach laptops to charts or kiosks.	Deters theft.	Does not prevent theft, only deters it.
Administrative Controls		
Develop policies and procedures regarding the acceptable use of computer equipment, including mobile devices with ePHI.	Policies and procedures, if enforced, may improve employee behavior and reduce risk incrementally.	Policies and procedures alone will probably not reduce risks sufficiently. Mistakes will still be made and there still could be loss and theft of laptops and other devices with ePHI.

[18] For additional information about alternatives to encrypting storage on end user devices see Appendix A of NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices, November 2007*

Possible Alternatives to Encryption		
Safeguard (Compensating Control)	Advantages/Strengths	Disadvantages/Weaknesses
Have the employee/user sign an "acceptable use agreement" that requires the user to acknowledge the "Acceptable Use Policy" before being provided with a mobile device and before allowing a personal device access to ePHI.	Acknowledgement of AUP may improve behavior and reduce risks incrementally.	The acknowledgement of AUP alone will probably not reduce risks sufficiently. Mistakes will still be made and there still could be loss and theft of laptops and other devices with ePHI.
Educate the workforce about the risks of lost or stolen laptops, smartphones and other removable media. Require safeguards such as not leaving a laptop unattended or where it might be easily stolen.	Education may improve behavior and reduce risks incrementally.	Education alone will probably not reduce risks sufficiently. Mistakes will still be made and there still could be loss and theft of laptops and other devices with ePHI.
Technical Controls		
Encryption of data at rest.	If encryption is properly implemented, sufficient encryption strength is used and the decryption key is protected by a strong password then encryption is very effective at preventing access to ePHI.	If the decryption password is discovered or if the secret key is not secured the encryption provides no protection. In addition if a device is lost or stolen after the data is decrypted then unauthorized access is possible.

Possible Alternatives to Encryption		
Safeguard (Compensating Control)	Advantages/Strengths	Disadvantages/Weaknesses
Remote wipe technology.	Can issue command to securely wipe all data from a storage device once the device has been reported lost or stolen.	The data is accessible until the remote wipe instruction is given.
RAID (redundant array of independent disks) storage.[19]	May make it difficult or even impossible to recover useful data from a single disk or partial set of disks used to store ePHI.	RAID is not intended to prevent access to data. It is intended to prevent loss of data if a single disk fails. It does not meet the legal standard for a safe harbor from the federal breach notification law.
Access controls such as user ID and password authentication.	Deters access via the operating system.	Does not prevent accessing the data as a secondary drive.

[19] RAID stands for redundant array of independent disks. It is a storage technology in which user data is stored redundantly on multiple disks. The redundant information is used to regenerate the user data in the event that one of the array's member disks or the access path to it fails. RAID is commonly used in data center storage arrays. (See: http://www.snia.org/education/dictionary/r)

Possible Alternatives to Encryption		
Safeguard (Compensating Control)	Advantages/Strengths	Disadvantages/Weaknesses
Information flow enforcement may be used to prevent ePHI from being copied to desktops, laptops and mobile devices. Six examples of this would be: 1) Configuring Microsoft Active Directory (AD) to relocate the "My Documents" folder to a network drive; 2) Using "thin client" technology to prevent data from caching[20] to the C drive; 3) Using AD policies or another tool to disable the ability to copy files to a USB drive; 4) Using Data Loss Prevention (DLP) software to detect or prevent the unauthorized movement of data; 5) Using network flow controls such as virtual local area networks (VLAN)[21] and access control lists (ACL)[22] to limit the flow of data across the network; 6) Disable the ability to write data to a CD/DVD or USB drive.	These safeguards can prevent specific flows of information and can be effective when combined with policies, training and enforcement. Some of these tools have a cost and also may be more effective when combined with encryption.	If these controls prevent or impede the user from doing their job they may seek to circumvent the safeguards. Many of these safeguards are not foolproof. For example, even if the My Documents folder is relocated to the network drive users will still have ways to save data to the C: drive. Also, it can take time to understand and control all of the ways that ePHI may flow to unauthorized devices.

From this analysis of compensating controls (safeguards) the following observations can be made:

[20] "Caching" refers to the temporary storage of a file on a disk drive. Web applications such as Outlook Web Access may create a copy of an attached file on the local PC hard drive when the attached file is opened. If the cached file contains sensitive information such as ePHI the cached file may create a security risk by its presence on the drive. For more information about how Outlook Web Access uses caching see http://technet.microsoft.com/en-us/library/bb885048(v=exchg.80).aspx

[21] A VLAN is a virtual network segment. VLANs are created in order to limit the flow of network traffic. Network components that are not on the same VLAN are not able to send and receive network packets to each other.

[22] An ACL is a list of rules within a network device, such as a router, that permit or prohibit the flow of network packets into and out of the network device.

- All of the listed safeguards have significant benefits to prevent unauthorized access to stored ePHI. Each of these safeguards should be considered as a component of a comprehensive security program.
- No single safeguard is without weaknesses. There is no silver bullet. Therefore, the best security posture is achieved by using multiple safeguards. Security professionals refer to this as "layered defense" or "defense-in-depth."
- Even encryption has potential weaknesses that must be understood and addressed through careful selection, configuration and support of encryption tools along with training on appropriate use.
- While administrative safeguards such as policies, training and asset management are essential, they do not provide sufficient protection for ePHI. Administrative safeguards should always be combined with technical and physical safeguards such as encryption, locked doors and passwords.

Conclusion

The CMS NPRM for Stage 2 gives the following explanation for its inclusion of this Core Measure and for the new emphasis on encryption of data at rest:

> This measure is the same as in Stage 1 except that we specifically address the encryption/security of data is that is stored in Certified EHR Technology (data at rest). Due to the number of breaches reported to HHS involving lost or stolen devices, the HIT Policy Committee recommended specifically highlighting the importance of an entity's reviewing its encryption practices as part of its risk analysis. We agree that this is an area of security that appears to need specific focus. Recent HHS analysis of reported breaches indicates that almost 40 percent of large breaches involve lost or stolen devices. Had these devices been encrypted, their data would have been secured. It is for these reasons that we specifically call out this element of the requirements under 45 CFR 164.308(a)(1) for the meaningful use measure. We do not propose to change the HIPAA Security Rule requirements, or require any more than would be required under HIPAA. We only emphasize the importance of an EP or hospital including in its security risk analysis an assessment of the reasonable and appropriateness of encrypting electronic protected health information as a means of securing it, and where it is not reasonable and appropriate, the adoption of an equivalent alternative measure.
>
> We propose this measure because the implementation of Certified EHR Technology has privacy and security implications under 45 CFR 164.308(a)(1). A review must be conducted for each EHR reporting period and any security updates and deficiencies that are identified should be included in the provider's risk management process and implemented or corrected as dictated by that process.[23]

The members of the HIMSS Risk Assessment Working Group agree with CMS that ongoing risk assessment is a critical step in protecting ePHI and that encryption of data at rest is in many cases a reasonable and appropriate safeguard—one is tempted to say, "a necessary" safeguard—and one that is still too often neglected. We hope this paper provides some valuable guidance to hospitals and eligible providers as they evaluate the security of their ePHI.

[23] Medicare and Medicaid Programs. Electronic Health Record Incentive Program, Stage 2, proposed rule. P 83.

References and Resources

HIPAA & Breach Enforcement
Statistics: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End-User Devices*, www.csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, www.csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf.

NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

NIST FIPS Publication 140-2 including Annex A, B, C and D; *Security Requirements for Cryptographic Modules,* http://csrc.nist.gov/publications/PubsFIPS.html

NIST Special Publication 800-111 - Guide to Storage Encryption Technologies for End User Devices http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

Work Group Contributors

This paper is a product of the HIMSS Risk Assessment Work Group. Its contributors include:

Work Group Chair
Jeffrey Bell, CISSP, CPHIMS, ACHE
CareTech Solutions

Work Group Contributors
Margaret Bond, MSc, MBA, CISM, CRISC, CHS-V
IASIS Healthcare

Nicholas Heesters, JD
Quality Insights of Delaware

Montra May, MBA
Georgia Department of Community Health

Glenn Mills, CIPP
SolveHIT.com

Jorge Rey
Kaufman, Rossin & Co.

David Scott St Laurent, CISSP, CISA, CISM
Fallon Community Health Plan

Protik Sandell
Potomac Data Systems Corp.

Dennis Seymour, CISSP, PMP
Ellumen

Louise Welch, CISA
Johns Hopkins University

HIMSS Staff
Lisa Gallagher, BSEE, CISM, CPHIMS, Senior Director, Privacy and Security

Mike Kroll, Associate Manager, Informatics