

Best Practices

A WHITEPAPER ON

HIPAA / HITECH REGULATORY COMPLIANCE

Inside this whitepaper:

- INTRODUCTION
- HIPAA, ARRA AND HITECH
- ENCRYPTION
- UNDER HIPPA WHY IS ENCRYPTION NECESSARY?
- WHAT KIND OF DATA NEEDS TO BE ENCRYPTED?
- HOW SHOULD THIS DATA BE ENCRYPTED?
- HOW DO YOU REALLY SECURE PHI?
- SECURITY ESSENTIALS FOR PRIVACY COMPLIANCE
- HIPAA SECURITY RULES BASICS



Loricca is a Service-Disabled Veteran Owned Small **Business**.

Introduction

This paper focuses on HIPAA compliance from the Security Rules perspective, and is intended to assist you in your ongoing compliance initiatives. The HIPAA Security rules are a very thorough and complicated set of regulations. In this section, we will explain the various components of the requirements in a straight-forward common sense fashion that will be easy to understand and help to move the overall organization toward a more secure environment with reduced risk while achieving compliance.


We will also discuss the various data control requirements that enable appropriate risk assessments, as well as prevention, protection, detection, and reaction to conditions that could adversely impact the confidentiality, integrity, and availability of information resources that either rely upon or could be adversely affected by a security breach with respect to the handling of information and the media on which information is contained.

HIPAA, ARRA and HITECH

On February 17, 2009, President Barack Obama signed a stimulus bill called the American Recovery and Reinvestment Act of 2009 (ARRA) into law. The "stimulus package" significantly expands HIPAA's privacy and security regulations.

Many of the security requirements can be met by creating guidelines, principles, templates, and checklists that are to be implemented and then used consistently throughout the enterprise (e.g., system, department, division) creating an efficient, consistent approach. Consistency will make the compliance initiative more understandable to the workforce and will help to justify the approach with regard to risk managers, external auditors, JCAHO, etc. Policy and procedures need to be either developed or updated, and then rolled out to the workforce via some type of training.

Much has been said and written about how to secure PHI under the HHS guidance and per various NIST guidelines for the purposes of meeting the "safe harbor" requirements. At the center of this discussion is the process of encrypting and destroying PHI, which is covered in the next section. The bottom line is that information owners and information custodians within your organization must ensure that information media containing PHI is stored in controlled location(s) where access is limited to people with a business need, subject to applicable legal, regulatory, or contractual restrictions.



*Security is
more than
a firewall*

Encryption

The encryption (*and destruction*) implementation specification applies to any medium that stores a covered entity's non-public information, including but not limited to, personal computers, servers, personal digital assistants, computer disks or CDs, DVDs, electronic tape, microfiche, film, and paper.

Encryption is a method of converting an original message (or data) of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text. Electronic protected health information falls into two basic categories; DAR and DIM; *data at rest* and *data in motion*, respectively. More on these is contained later in this section.

The HIPAA Security Rule allows organizations to choose the type of encryption they will use. Adequate encryption for HIPAA should mean that the software makes use of seasoned encryption algorithms which can't be penetrated by someone with dedicated tools or governmental deciphering resources, if at all. Examples of these include DES, AES, RSA, Blowfish, Twofish, etc. Other encryption solutions include Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), Virtual Private Networks (VPN), secure FTP, Secure Shell (SSH), and Pretty Good Privacy (PGP) or similar encryption products for encrypting e-mails. No algorithm will guarantee total security against the various types of security attacks that professional hackers can employ, but adequate encryption for the majority of business and regulatory compliance purposes is available via many free or inexpensive products, including:

- Abi-Coder at <http://www.abisoft.net/oldCoder.html>. This site also includes some excellent papers on security and encryption. You can also purchase the most recent versions of Abi-Coder and Abi-SecurePro at this site.
- MaxCrypt at <http://www.tucows.com/preview/195463.html> - inexpensive and fast.
- WinZip at <http://www.winzip.com> -- a must have. Adds encryption to compression.
- BestCrypt and BCWipe at <http://www.jetico.com>
- AxCrypt at <http://axcrypt.sourceforge.net>
- FineCrypt at <http://www.finecrypt.net>. There is a good paper available at this site entitled "An Introduction to the Use of Encryption".
- Encrypted Magic Folders at <http://www.pc-magic.com/des.htm> -- *"...gives you automated and transparent encryption. Select folders whose files you want encrypted and EMF not only makes those folders and files completely invisible to others but decrypts and encrypts the files automatically and transparently as you use them. You won't even know you're using encrypted files as EMF does all the work behind the scenes."*



Under HIPAA why is encryption necessary?

The Section 164.530(c) of the HIPAA Privacy Rule states the following:

1. Standard: safeguards. A covered entity must implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.
2. Implementation specification: safeguards i) a covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Email is not totally secure: The main risk when sending email is the deliberate interception of the message by an unauthorized individual, or "hacker". This person could read, interchange, or delete the message. Another more common risk, however, is the unintentional emailing of information to an incorrect recipient. In both of these examples, an unauthorized individual has access to identifiable medical information that was not intended for them, so an unintentional or incidental disclosure is occurring. Encryption is a technical safeguard you can use to protect data from these risks.

What kind of data needs to be encrypted?

All PHI needs to be encrypted. Under HIPAA, PHI includes immunization information that is individually identifiable. Another common question in this area is "Who needs to encrypt data and when do they need to encrypt it?" and the safest answer is, everyone emailing PHI should encrypt the data every time they send it.

How should this data be encrypted?

All PHI data that is to be emailed should be encrypted with a strong encryption algorithm, which protects sensitive information with a digital key. This key is a digital combination lock that can only be unlocked by the recipient of the email message. The US government has approved an algorithm called the Advanced Encryption Standard (AES) for its own use, so AES is a good choice.

Does the HIPAA Security Rule allow for sending e-PHI in an email or over the Internet? If so, what protections must be applied?

The Security Rule does not expressly prohibit the use of email for sending electronic PHI. However, the standards for access control, (45 CFR § 164.312(a)) integrity (45 CFR § 164.312(c) (1)), and transmission security (45 CFR § 164.312(e) (1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against the unauthorized access to electronic PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect electronic PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for electronic PHI to be sent over an electronic open network as long as it is adequately protected.

Do the HIPAA Security Rule requirements for access control, such as automatic logoff, apply to employees who telecommute or have home-based offices if the employee accesses electronic protected health information (PHI)?

Yes. Covered entities that allow employees to telecommute or work out of home-based offices and have access to electronic PHI, must implement appropriate safeguards to protect the organization's data. The automatic logoff implementation specification is addressable, and must therefore be implemented if, after an assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its environment. If the entity decides that the logoff implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate, or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure.

The information access management and access control standards, however, require the covered entity to implement policies and procedures for authorizing access to electronic PHI and technical policies and procedures to allow access only to those persons or software programs that have been appropriately granted access rights.

What is the difference between Risk Analysis and Risk Management in the HIPAA Security Rule?

Risk analysis is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic PHI held by a covered entity, and the likelihood of occurrence. The risk analysis may include inventorying of all systems and applications that are used to access and house data, and classifying them by level of risk. A thorough and accurate risk analysis would consider all relevant losses that would be expected if the security measures were not in place, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage. Risk management is the actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its electronic PHI and to meet the general security standards.

What is system vulnerability?

A system vulnerability is a flaw or weakness in a system, due to its design, installation, lack of policies and procedures, or some other cause. Any of these weaknesses, whether intentional or accidental, could potentially result in a breach or inappropriate use or disclosure of e-PHI. Some vulnerabilities may be caused by ineffective policies regarding user or logon IDs and passwords, holes or weaknesses in some of the software tools, or flaws in the operating system, application or inadequate access controls.

How will we know if our organization and our systems are compliant with the HIPAA Security Rule's requirements?

The purpose of the final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of e-PHI that is collected, maintained, used or transmitted by a covered entity. Compliance is different for each organization and no single strategy will serve all covered entities. Covered entities should look to § 164.306 of the Security Rule for guidance to support decisions on how to comply with the standards and implementation specifications contained in §§ 164.308, 164.310, 164.312, 164.314, and 164.316. In general, this includes performing a risk analysis; implementing reasonable and appropriate security measures; and documenting and maintaining policies, procedures and other required documentation. Compliance is not a one-time goal, it must be maintained. Compliance with the evaluation standard at § 164.308(a) (8) will allow covered entities to maintain compliance. By performing a periodic technical and nontechnical evaluation a covered entity will be able to address initial standards implementation and future environmental or operational changes affecting the security of electronic PHI.

Are we required to “certify” our organization’s compliance with the security standards?

No, there is no standard or implementation specification that requires a covered entity to “certify” compliance. The evaluation standard § 164.308(a) (8) requires covered entities to perform a periodic technical and nontechnical evaluation that establishes the extent to which an entity’s security policies and procedures meet the security requirements. The evaluation can be performed internally by the covered entity. There are also external organizations that provide evaluations or “certification” services. A covered entity may make the business decision to have an external organization perform these types of services. It is important to note that HHS does not endorse or otherwise recognize private organizations’ “certifications,” and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a “certification” by an external organization does not preclude HHS from subsequently finding a security violation.

Does the Security Rule apply to written and oral communications?

No. The Security Rule is specific to electronic PHI. It should be noted however that electronic PHI also includes telephone voice response and faxback systems because they are used as input and output devices for computers. Electronic PHI does not include paper-to-paper faxes or video teleconferencing or messages left on voice mail, because the information being exchanged did not exist in electronic form before the transmission. In contrast, the HIPAA Privacy Rules address all mediums of PHI, including written and oral.

What does the HIPAA Security Rule mean by physical safeguards?

Physical safeguards are physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security, and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity’s premises or at another location.

Does the HIPAA Security Rule mandate minimum operating system requirements for the personal computer systems used by a covered entity?

No. The Security Rule was written to allow flexibility for covered entities to select the technology that best fits their organizational needs. The Security Rule does not specify minimum requirements for personal computer operating systems, but it does mandate requirements for information systems with electronic PHI. Therefore, as part of the information system, the security capabilities of the operating system may be used to comply with technical safeguards standards and implementation specifications such as audit controls, unique user identification, integrity, person or entity authentication, or transmission security.

Are covered entities required to use the National Institute of Standards and Technology (NIST) guidance documents referred to in the preamble to the final HIPAA Security Rule?

No. Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.

What is Public Key Infrastructure (PKI)?

Public key infrastructure is the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke Public Key Certificates based on public key cryptography.

What is a Digital Signature?

A Digital Signature is a type of electronic signature that combines a one-way secure hash function with public key cryptography to provide data integrity (assuring that the data has not been altered) and non-repudiation (assuring that the signer cannot later deny signing the document or message). However, a digital signature does not provide confidentiality for the signed document or message because a Digital Signature does not encrypt the document or message.

How do You REALLY Secure PHI?

This is the big question many healthcare entities and their business associates are asking. The reason for the question is the wording in the Health Information Technology for Economic and Clinical Health Act (HITECH) of the American Recover and Reinvestment Act of 2009 (ARRA). In 2009, a document was developed and released by HHS with the partial title containing "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act. . ." It's a long title, but the document is actually helpful once you understand its content, which can be viewed in its entirety using the following link: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf>.

The HITECH Act required HHS to issue interim final regulations, spelling out the requirements of covered entities and business associates to plan and provide for notification in the case of breaches of unsecured PHI.

The breach notification requirement applies to any HIPAA covered entities and business associates that access, modify, record, store, destroy or otherwise use or disclose unsecured PHI. It is important at this point to note that if PHI is rendered unidentifiable or information is de-identified, these data records are outside the scope of the breach notification requirement, because now the information is no longer classified as PHI. Additionally, PHI that is not considered electronic (or e-PHI), meaning PHI that is contained on portable storage devices, removable disks or even paper, are sometimes called hard media, and this data is most certainly covered by the rules. Hard copy paper PHI, or other hard media, is determined to be secured via its destruction.

HHS has continued to remind covered entities that all other aspects of HIPAA still apply, for both the privacy and security rules, and wants to make the point that the latest guidance simply serves as *the functional equivalent of a safe harbor*.

DAR / DIM

With respect to the breach notification requirements, some HIPAA-covered entities have made the wrong assumption that they only need to worry about 'data in motion' (DIM) and can relax when it comes to 'data at rest' (DAR). HHS makes the distinction between data in motion, which is data travelling through a network such as a wireless transmission, and data at rest, which pertains to data that resides in storage devices/systems like structured databases and file systems. HHS makes a point to note that the methods for rendering DAR/DIM PHI unusable, unreadable or indecipherable to unauthorized individuals must have the same application when referring to both data in motion and data at rest.

There was a time when USB keys—aka thumb drives, flash tokens, or keychain drives—were simple storage devices that helped you carry a file or two around with you. The size was nice, but they weren't really much better than a high-tech floppy disk when they first came out. My, how things have changed. USB is an acronym for *Universal Serial Bus*. Now, there are many types of USB keys that are available: conventional flash drives, U3 flash drives, and small hard drives. Simple *flash drives* can hold one or two gigabytes of data. *USB hard drives* can offer as much as 6GB of plug-and-play storage, letting you carry an entire library of data and important documents wherever you go. Now, a new generation of "*smart*" *flash drives* is using the U3 platform to deliver entire applications on a single USB key. Plug a U3 key into any system and you can use your browser, e-mail client, and applications as if they were loaded on that system. Unplug it, and there is no trace of you or your software on the system. This is why CMS is looking at these devices very closely.

Safe Harbor: Encrypt or Destroy

PHI is typically secured in two ways; if it is either encrypted or destroyed. HHS notes that other methods may also suffice, but their guidelines identify only these two methods, with some specific guidance attached to each. NIST publications give good ideas and methods on how to encrypt EPHI, and it would be beneficial to use these guidelines.

With regard to DAR, valid encryption processes are consistent with NIST Special Publication number 800-111, entitled "**Guide to Storage Encryption Technologies for End User Devices**" which came out in November 2007. It is available via the following link: <http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf>.

With regard to DIM, valid encryption processes are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include the standards that have been described in NIST Special Publications 800-53, Guidelines for Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or Special Publication 800-113, Guide to SSL VPNs. Also, we must mention that others may be included later once they conform to FIPS 140-2 requirements.

The links for these documents are:

NIST 800-52: <http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf>

NIST 800-77: <http://www.csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf>

NIST 800-113: <http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf>

FIPS 140-2: <http://csrc.nist.gov/publications/PubsTC.html>

Security management and risk mitigation is an ongoing process. However, to get a good baseline start towards a secure environment, certain steps must be carried out.

Michael Whitcomb, PMP, CISM

Michael is the founder and President of **Loricca, Inc.** He has 25 years of experience building and supporting secure systems for government and commercial organizations of all sizes. Michael brings the technical knowledge and proven leadership ability for Loricca to provide world class security services. Since founding Loricca, Michael has established the company's presence providing security solutions to some of the country's largest companies.

Prior to Loricca, Michael served in technical leadership positions, leading and implementing solutions for various clients within both the government and commercial sectors including finance, healthcare, retail and federal government. Michael holds a Bachelor of Science in Management of Information Systems from the University of Phoenix in addition to the PMP and CISM professional certifications.

Loricca's goal in providing the information in the expanded version of this document is to provide HIPAA/HITECH covered entities and business associates with practical solutions and guidelines showing what steps can/should be taken in moving toward a fully compliant organization and reducing overall risk to the enterprise.

Loricca, Inc. | www.loricca.com | 813.600.3005 | mwhitcomb@loricca.com

