HIPAA Requirements for Encryption

A White Paper from SafeLogic

SafeLogic Inc.

530 Lytton Ave, Suite 200

Palo Alto, CA 94301

www.SafeLogic.com

Executive Summary

The creation of the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was a landmark step for the US health care system. Designed in part to stimulate the growth and effectiveness of electronic patient data interchange, standards were put in place to increase efficiency and to protect the privacy of the participating individuals. As with most federal regulations on technology, special attention was given to the need for encryption of sensitive data. Beyond the implementation of complex algorithms, properly securing Electronic Protected Health Information (ePHI) demands compliance with Federal Information Processing Standard (FIPS) 140-2. This is a time-consuming and difficult validation process. Standard approaches to integrate encryption routines into custom software have resulted in increased development time, conflicting with the time constraints of end customers. Products often deploy late or without validated encryption routines. SafeLogic's 'Drop-In Compliance' approach provides a crypto module that meets customer demand for both validation and short development time. This paper presents the encryption requirements for use in accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and discusses the benefits of SafeLogic's CryptoComply module.

Table of Contents

1 HIPAA / HITECH Requirements

The Health Information Technology for Economic and Clinical Health (HITECH) Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require "covered entities" and "business associates" to implement and manage an information security program. Table 1 provides a summary of the major documents of that specify the HIPAA security and privacy requirements for Protected Health Information (PHI).

Document	Title	Description
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act	Part of the American Recovery and Reinvestment Act of 2009 (ARRA) that strengthens the privacy and security protections for Health Information Portability and Accountability Act (HIPAA).
HIPAA Security Rule	Security Standards for the Protection of Electronic Protected Health Information	Establishes the national set of security standards for the handling of Protected Health Information in electronic form (ePHI).
HIPAA Privacy Rule	Standards for Privacy of Individually Identifiable Health Information	Establishes the national standards for the handling of Protected Health Information (PHI).
NIST SP 800-66	An Introductory Resource Guide for Implementing the HIPAA Security Rule	Voluntary guideline and best practices for implementation of HIPAA security rule.
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations	Federal guideline for selecting the minimum-security controls for information systems and the organization.

FIPS 140-2	Security Requirements for Cryptographic Modules	Federal standard for the specification of cryptographic-based security systems used to protect sensitive data. Also established the Cryptographic Module Validation Program (CMVP) for the validation of cryptographic modules by Cryptographic and Security Testing (CST) laboratories.
FIPS 140-3 DRAFT	Security Requirements for Cryptographic Modules	Proposed revision for FIPS 140-2

Table 1. HIPAA Security and Privacy Implementation Documents. *The Health Information Portability and Accountability Act (HIPAA) Security and Privacy rules establish minimum protection requirements for Protected Health Information (PHI). The National Institute of Standards and Technology (NIST) Special Publications 800-66, 800-53 and the Federal Information Processing Standards (FIPS) provide additional guidance on the implementation of those controls.*

1.1 Required and Addressable HIPAA Security Controls

Covered entities, organizations that transmit health information in connection with billing and payment for health services or health insurance coverage, are required to meet the minimum security controls as specified in the HIPAA Security Rule. These controls are designated either as "Required" or "Addressable". Required controls must be implemented as stated, while addressable controls may be treated as follows:

- The control is implemented as stated.
- If the control is unreasonable or inappropriate for the environment, an alternative control accomplishing the same purpose must be implemented.
- If there is no reasonable or appropriate alternative, then no control is implemented, but the decision must be documented in a security risk analysis.

In this paper, we will indicate addressable controls, but we will discuss them as if the covered entity intends to implement the control as stated. Although it is possible to assess each addressable control individually, NIST SP 800-66 points out that "for federal agencies, however, all of the HIPAA Security Rule's addressable implementation specifications will most likely be reasonable and appropriate safeguards for implementation, given their sizes, missions, and resources." We will make the same assumption, and treat each control as though it must be addressed.

1.2 NIST SP 800-66 Interpretation

The HIPAA Security Rule gives us little guidance in the implementation of cryptographic controls. For example, HIPAA 164.312(e)(2)(ii) states, "Encryption (Addressable): Implement a mechanism to encrypt [Electronic Protected Health Information] whenever deemed appropriate." As a result, NIST created a special publication, NIST SP 800-66: *An Introductory Resource Guide for Implementing the HIPAA Security Rule*, to provide greater depth and breadth to these controls by mapping the HIPAA security controls to a standard security controls framework (NIST SP 800-53). By following this protocol, we can demonstrate the current guidance for the use of validated cryptographic modules in situations governed by HIPAA.

NIST SP 800-53 cryptographic controls require the use of validated cryptographic modules. NIST considers systems that use unvalidated cryptography to be equal to those providing no cryptographic protection at all. Thus, a FIPS 140-2 validated module should be leveraged to meet NIST SP 800-53 and HIPAA requirements.

The Cryptographic Module Validation Program (CMVP) was established by NIST in association with their Canadian counterpart, CSEC, to validate cryptographic modules that meet FIPS 140-2 security standards. Vendors of cryptographic modules use independent and accredited Cryptographic and Security Testing (CST) laboratories to test their modules and qualify for the validation. Without the guidance and validation provided by NIST, HIPAA and other legislation would fail to uphold the intended privacy and encryption standards.

2 HIPAA/NIST SP 800-66 Encryption Requirements

The minimum security requirements for information systems of the covered entities are documented in the HIPAA Security Rule and interpreted by the NIST SP 800-66 publication.

Limiting our discussion to the encryption requirements and other security requirements directly affected by encryption, there are thirteen (13) controls in which encryption is addressed within the HIPAA Security Rule. Some of the requirements specifically address encryption, while others allow for encryption to be used as a mechanism to support or enhance a security control. In all cases, if encryption is employed as a mechanism to meet a security requirement, this NIST guideline states that it must be FIPS 140-2 compliant and validated under the Cryptographic Module Validation Program (CMVP).

There are five (5) required HIPAA security controls addressed by cryptographic techniques and eight (8) addressable HIPAA security controls addressed by cryptographic techniques. Table 2 displays these controls mapped to the appropriate control in NIST SP 800-53, as specified in NIST SP 800-66.

HIPAA Security Ref.	Control Name	NIST SP 800-53 Control
Encryption		
164.308(a)(5)(ii)(D)	Password management (A)	IA-7
164.312(a)(2)(iv) 164.312(e)(2)(ii)	Encryption and Decryption (A) Encryption (A)	SC-13
Data at Rest		
164.310(d)(1)	Device and Media Controls (R)	MP-4 (1)
Data in Transmission		
164.310(d)(1) 164.312(c)(1)	Device and Media Controls (R) Integrity (R)	MP-5 (4)
164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(i)	Integrity (R) Mechanism to Authenticate ePHI (A) Integrity Controls (A)	SC-8 (1)

164.312(e)(1) 164.312(e)(2)(ii)	Transmission Security (R) Transmission Security – Encryption (A)	SC-9 (1)
Access Control		
164.308(a)(3)(ii)(A) 164.308(a)(4)(ii)(B) 164.312(a)(1) 164.312.(a)(2)(iv)	Authorization and Supervision (A) Access Authorization (A) Access Control (R) Encryption and Decryption (A)	AC-3 (6)
164.310(d)(1) 164.312(c)(1)	Device and Media Controls (R) Integrity (R)	MP-2 (2)
Identification and Authentication		
164.312(d)	Person or Entity Authentication (R)	IA-3(1) (2)
164.310(d)(1)	Device and Media Controls (R)	MP-4 (1)

Table 2. HIPAA Security Controls Addressed by Encryption. *The five required and eight addressable HIPAA security rule requirements that involve cryptographic techniques as mapped to NIST SP 800-53, according to NIST SP 800-66.*

3 NIST SP 800-53 Encryption Controls

As shown in Table 2, the thirteen HIPAA security controls (five required and eight addressable) map to nine appropriate controls in NIST SP 800-53. The protocols of NIST SP 800-66 provide for several controls, but these are specific to encryption. By using a FIPS 140-2 validated cryptographic module, these nine controls are satisfied.

They have been organized into five categories: Encryption, Data at Rest, Data in Transmission, Access Control, and Identification and Authentication. You may notice that certain HIPAA requirements have been mapped to several NIST SP 800-53 controls, and some NIST controls address several HIPAA requirements.

Here is a brief description of each of the controls specified in NIST SP 800-53.

3.1 Encryption

The following security requirements directly address the use of encryption technology in federal systems.[1]

IA-7 Cryptographic Module Authentication

The cryptographic module within the information system must implement authentication mechanisms (i.e., role-based or identity-based) to control access to the cryptographic module.

SC-13 Use of Cryptography

For any cryptographic protection for policy enforcement within the information system the cryptographic modules implementing those services and protections must comply with federal laws (i.e., FIPS 140-2 and the CMVP).

3.2 Data at Rest

The following security requirements utilize encryption technology in federal systems to protect sensitive data stored on information systems and components.

MP-4 (1) Media Storage

The organization employs cryptographic mechanisms to protect information in storage.

[1] A family identifier (two-characters assigned to uniquely identify the security control family), and a numeric identifier (one or two digits assigned to indicate the control number within the family) is assigned to each requirement. A complete listing of all control families and controls can be found in NIST SP 800-53.

3.3 Data in Transmission

The following security requirements utilize encryption technology in federal systems to protect sensitive data transmitted on information systems and components.

MP-5 (4) Media Transport

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

SC-8 (1) Transmission Integrity

The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

SC-9 (1) Transmission Confidentiality

The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

3.4 Access Control

The following security requirements utilize encryption technology in federal systems to prevent unauthorized access to sensitive information on information systems and components.

AC-3 (6) Access Enforcement

The organization encrypts or stores off-line in a secure location.

MP-2 (2) Media Access

The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.

3.5 Identification & Authentication

The following security requirements utilize encryption technology in federal systems to authenticate the credentials of active entities in support of identification-based access control.

IA-3 (1) (2) Device Identification and Authentication

The information system authenticates devices before establishing remote, wireless network, and network connections using bidirectional authentication between devices that is cryptographically based.

4 Conclusion

As a software developer, you are aware that covered entities demand custom-developed enterprise and mobile applications for a diverse set of mission needs, but information security is always among the top requirement. HIPAA compliance requires particular attention to the cryptographic functions to ensure privacy and protection of patient health information.

In order to meet the HIPAA Security Rules, NIST demands the use of a validated cryptographic module in the implementation of the cryptographic requirements. They provide the guidance and directions to address HIPAA requirements, and their stance on cryptographic modules is clear: either it is validated to FIPS 140-2 standards, or it is unacceptable.

SafeLogic's CryptoComply meets all encryption requirements set forth by HIPAA. By leveraging a 'Drop-In Compliance' approach, SafeLogic accelerates the timeline for integration, reduces the overall development time and eliminates compliance risks. FIPS 140-2 is a challenging and time-consuming process and can be a major distraction to engineering teams. While traditional methods require significant commitment of time and resources, developers can integrate CryptoComply quickly and return to their core tasks. The net result is that developers are able to maintain focus on the product while compliance is achieved immediately.

The barrier to entry for HIPAA compliant products is high for good reason. FIPS 140-2 has traditionally posed a significant roadblock but now offers an opportunity for competitive advantage. The solutions that integrate CryptoComply will enjoy instant compliance, faster release cycles, and the ability to sell the current product as FIPS 140-2 compliant. Waiting 12 months or longer to receive FIPS 140 validation will quite simply render a product irrelevant, no matter the quality of engineering. Covered entities need solutions that are compliant *now*.

In conclusion, be aware of the HIPAA compliance demands of end users and begin planning a strategy as soon as possible. Please don't hesitate to reach out with questions regarding CryptoComply or the encryption requirements of HIPAA.

4.1 About SafeLogic

SafeLogic's product line is focused on standards-based cryptographic engines designed for use in Cloud, mobile, wearable, IoT, server, workstation, and appliance environments. These modules have been fully validated to FIPS 140-2 standards and offer drop-in OpenSSL and Bouncy Castle compatibility, a variety of connectors to accommodate unique product architecture, and instant compliance for federal deployments to SafeLogic customers.

Even better, SafeLogic modules include RapidCert, the industry's only FIPS 140-2 validation service that provides a certificate in the customer's name, while drastically accelerating the timeline, requiring no additional engineering effort, zero interaction with testing labs, and at a fixed cost.

SafeLogic's customers are among the most influential and innovative companies in technology today, from startups to the Fortune 100.

SafeLogic was established in 2012, is privately held and is headquartered in Palo Alto, California.

SafeLogic

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301

(844) 4-ENCRYPTION

www.SafeLogic.com

www.Twitter.com/SafeLogic