Impero

Connect
Fast, Secure Remote Access

HIPAA Compliance Checklist

Concerned about security compliance for your remote access solution? Here is how Impero helps you meet even the toughest standards.

What is HIPAA?

Organizations that must adhere to the Health Insurance Portability and Accountability (HIPAA), know that encryption is now a de facto primary aspect of HIPAA compliance after the passing of the HITECH Act.

There are a couple of reasons for this increased focus on encryption.

First, the U.S. Department of the Health and Human Services (HHS) issued guidance wherein "unsecure protected health information (PHI)" is essentially any PHI that is not encrypted or destroyed. Under this definition, it doesn't matter how many chains, walls, doors, biometric gizmos and guards with lethal weapons you have at your service. As long as PHI is not encrypted, it is considered unsecured.

A second and more compelling reason why encryption is now a requirement is the introduction of HITECH's breach notification initiative, which requires HIPAA-covered entities to send notification letters if there is a breach of unsecured PHI. However, as HHS pointed out, the use of encryption grants safe harbor in the event of a breach because encrypted PHI is not unsecured PHI.

Oddly enough, in the same breath, HHS also notes that "covered entities and business associates are not required to follow the guidance." However, cleaning up the mess behind a breach notification can cost millions of dollars, so one would have to be supremely confident — or reckless — in not taking advantage of the encryption safe harbor. With such mixed signals, though, it is not hard to see why encryption is called a de facto requirement.

What type of encryption is required?

In the past, companies offered hard drives that used strong encryption. However, analysis showed that strong encryption was used but only to protect the password and not the data that was stored on the devices. The actual data stored on the hard drive was encrypted with an encryption algorithm developed by the company, which proved to be anything but strong.

This illustrates the potential pitfalls of choosing any type of encryption package — a lack of strong, secure encryption. Obviously, some applications do a better job of protecting data than others, but how can a company choose the right one?

HHS does not provide any guidance in this area. Instead, HHS defers to the National Institute of Standards and Technology (NIST) to direct organizations to a number of special publications on the subject.

While these requirements are for federal agencies, they could also serve as a great guide for private practices. Since HHS deferred to NIST when it comes to encryption, companies need to meet the expectations of what NIST considers "proper" encryption for sensitive data.

Data at motion

Data in motion refers to data going through networks. Encrypting data in motion is straightforward: Valid encryption processes must "comply with the requirements of Federal Information Processing Standards (FIPS) 140–2." While there are many technical requirements involved, finding a vendor that offer products that are FIPS 140-2 compliant, is the solution.

Data at rest

Data at rest refers to data that is stored on servers, desktops, laptops, external hard drives, CD's, DVD's, backup tapes etc. Finding appropriate data at rest encryption requires a little digging. According to the suggested NIST publication — Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices — "Federal agencies must use FIPS-approved algorithms contained in validated cryptographic modules. Whenever possible, AES (Advanced Encryption Standard) should be used for the encryption algorithm because of its strength and speed."

Also, a footnote makes reference to NIST SP 800-57, "Recommendation for Key Management," and notes that it "provides detailed information on key management planning, algorithm selection and appropriate key sizes, cryptographic policy and cryptographic module selection."

This information is relegated to a footnote. This is unfortunate since this publication is what most HIPAA-covered entities are looking for. As organizations review section 5.6.2 of the publication, they can identify encryption algorithms that are valid for use, the minimum key sizes and the length of their validity. In addition, examples are given on how all of the above comes together, and summarized in a table. Any encryption weaker than this, and you might not be covered.

HIPAA-covered entities can expect safe harbor if, and only if, they adhere to these strict standards and guidelines. The fact that a company's data is encrypted is meaningless without taking into account the NIST requirements. Organizations that properly adhere to HIPAA standards understand the impact of breach notifications. By proactively leveraging the proper encryption technologies, companies of all sizes can avoid these breach notifications while ensuring the security of their sensitive data.

Security Requirements	How Impero Connect meets them
NIST Special Publication 800-66[1]. Descriptions. HIPAA Safeguard R=Required / A=Addressable	
Access Control (R): 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 as specified in § 164.308(a)(4). [164.312(a)(1)]	**Centralized 2 and 3 Factor Authentication** **Impero Authentication via Security Server** The Impero Security Server verifies the guest identity against the database service that holds all the pre-defined guest IDs and passwords. **Windows Authentication via Security Server** The Impero Security Server verifies the guest identity by letting the host relay the authentication process to a Windows domain controller. **Directory Service Authentication via Security Server** The Impero Security Server verifies the guest identity against a directory service via LDAP. **RSA securID with 'Triple-Factor Authentication' via Security Server** The Impero Security Server combines RSA SecurID 'two-factor authentication' with a shadow Impero guest ID password.
Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity. [164.312(a)(2)(i)]	**Centralized 2 and 3 Factor Authentication (see above)** Impero can be set to terminate a session after a timeout period and be instructed to lock the computer automatically. *See the table on the following page...
Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. [164.312(a)(2)(iii)]	
Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. [164.312(a)(2)(iv)]	
Audit Controls (R): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronically protected health information. [164.312(b)]	**Impero Logging** Impero can record all sessions verbatim to document the entire remote session. Impero Security Server provides a central log with more than 100 events and stores this information in an ODBC-compliant database for maximum security and scalability. Log data can be kept for an unlimited time along with the physical support session providing complete audit and playback capabilities.
Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. [164.312(c)(2)]	
Log-in Monitoring (A): Procedures for monitoring log-in attempts and reporting discrepancies. [164.312(a)(5)(ii)(C)]	

Person or Entity Authentication (R): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. [164.312(d)]

Smart Card Authentication and Tunneling

By using a Smart Card and a Smart Card reader at the windows guest, the windows host is now able to authenticate the identity of the guest user via the Security Server that communicates with a Windows server with Microsoft CA installed. If the host computer demands local logon using Smart Card the guest user's credentials will be tunneled to the host in order to provide the information.

Transmission Security (R): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. [164.312(e)(1)]

*See table below

Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. [164.312(e)(2)(ii)]

*See table below

Encryption

Data transmitted between Windows, Linux, Solaris and Mac OS X modules can be encrypted using the Advanced Encryption Standard (AES – FIPS 197) with key lengths up to 256-bits.

Integrity and message Authentication

Verified using the Keyed-Hash Message Authentication Code HMAC SHA-1 (FIPS 198- 1/FIPS 180-3) or HMAC SHA-256 (FIPS 198-1/FIPS 180-3) based on the Secure Hash Standards SHA-1(FIPS 180-3) or SHA-256 (FIPS 180-3).

Key exchange

Encryption keys for encrypted data transmissions are exchanged using the Diffie-Hellman method (SP 800-56 A) with key lengths up to 2048 bits and up to 256-bit AES (FIPS 197) and up to 512-bit SHA HMAC (FIPS 198-1/FIPS 180-3) verification.

Algorithms used by Impero Connect

Type	Algorithm	FipS 140-2 Approved
Key Exchange	Diffie-Hellman	Yes - SP 800-56 A
Symmetric Key	AES (Key sizes: 128-256)	Yes – FIPS 197
Digest	SHA-1 SHA-256 SHA-512	Yes – FIPS 180-3 Yes – FIPS 180-3 Yes – FIPS 180-3
Message Authentication Code	HMAC SHA-1 HMAC SHA-256 HMAC SHA-512	Yes – FIPS 198-1/FIPS 180-3 Yes – FIPS 198-1/FIPS 180-3 Yes – FIPS 198-1/FIPS 180-3

RSA SECURED®
RSACERTIFIED

Impero