ENCRYPTION
OF CLOUD DATA

OnLINE TECH

Table of Contents

1.0. Executive Summary

Organizations seeking to protect sensitive and mission-critical data quickly realize that there is no single answer to keep all systems completely secure. Online data security is a complex, rapidly evolving landscape, requiring robust and layered protections. Encryption is one tool in a comprehensive defense-in-depth strategy to mitigate the risk of accidental and intentional data breaches.

Like every other technology tool, implementation must work within a broader digital ecosystem, without disrupting the purpose that the system was designed to fulfill. Evaluating the benefits of encryption against potential tradeoffs such as cost, performance, and ongoing maintenance is at the heart of determining the most effective and efficient means of using encryption.

First, a few basics:

What is encryption?

Encryption takes plaintext (your data) and encodes it into unreadable, scrambled text using mathematical algorithms, effectively rendering data unreadable unless a cryptographic key is applied to convert it. Encryption ensures data security and integrity, even if accessed by an unauthorized user, provided the encryption keys have not been compromised. Encryption can protect data in motion, referred to encryption in transit or encryption in flight, as well as at rest; meaning in storage. Encryption often occurs at multiple levels of a system, appropriate to the context of use and other system components.

Why use encryption?

Encryption is considered a best practice for any security-conscious organization, including those that need to meet specific industry compliance requirements such as HIPAA compliance for healthcare, PCI DSS compliance for ecommerce and retail, and SOX for financial reporting. Recurring data breaches are increasing, particularly in the healthcare industry that reports an estimated $7 billion loss due to data breaches.[1]

Even those organizations that determine their risk of data loss is minimal often choose encryption to mitigate the risk of having to report a data breach, since the loss of encrypted data may not be considered a reportable event if the encryption keys remain safe.

The increased cyber threats of hackers and data theft presents a strong case for employing encryption and infrastructure that both secures data while delivering strong computing performance for optimal data availability and reliability. In this white paper, different types of encryption will be discussed, including using encryption in the cloud.

[1] Online Tech & The Ponemon Institute; *Healthcare Industry Loses $7 Billion Due to HIPAA Data Breaches*

Although encryption is *not* a silver bullet of data or system security, it is one key tool that can be accompanied by a full arsenal of security services for a layered-defense approach to ensuring data is protected, even if accessed by unauthorized individuals. Additional security options to add to your IT solution will be covered.

2.0. Encryption for Compliance

2.1. HIPAA Encryption

Healthcare organizations (also called covered entities or CEs), business associates (BAs) and subcontractors that support the facilitation, processing or collecting of protected health information (PHI) must comply with the Healthcare Insurance Portability and Accountability Act (HIPAA) and HITECH Act enforced by the U.S. Department of Health & Human Services (HHS).

With addressable encryption implementation specifications, both a covered entity and business associate must consider implementing encryption as a method for safeguarding electronic protected health information (ePHI). If encryption is not used by a covered entity or business associate, clear documentation of the risk analysis, the decision not to encrypt, and the specifics of an equivalent level of protection must be in place to prove due diligence to protect ePHI.

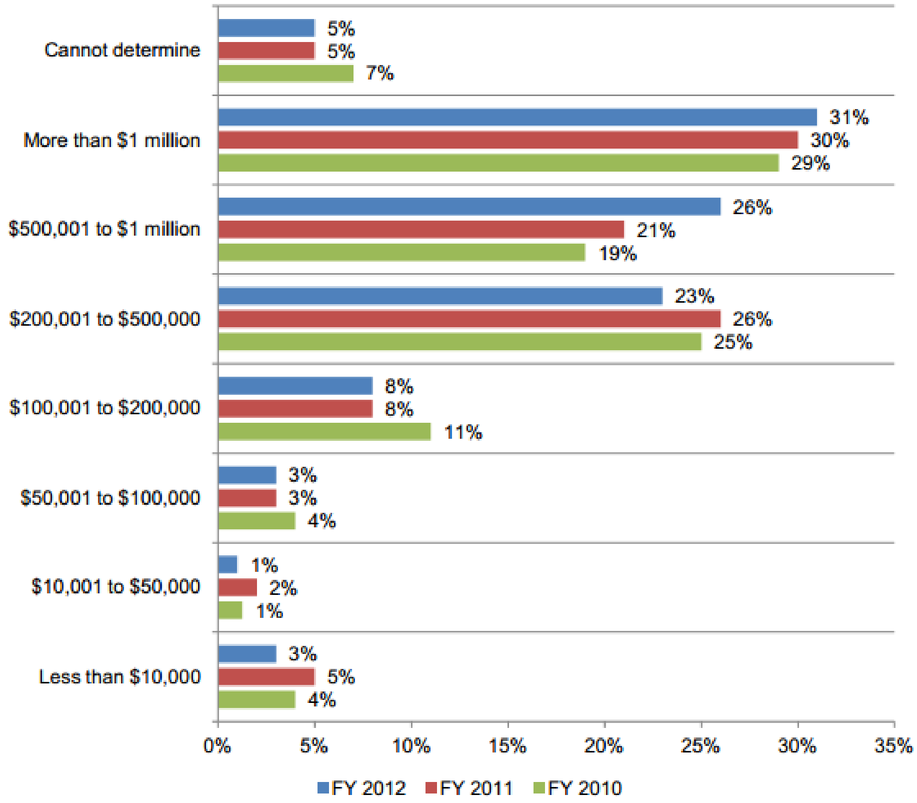
Even when equivalent protection is possible, many organizations opt to encrypt to save on the costs of publically announcing and remediating a data breach, as encrypted data is not considered compromised if the encryption keys remain safe. This means a stolen laptop with patient records is not a reportable event if the PHI is encrypted, and the encryption keys remain safe.[2]. The costs of a data breach involving ePHI is one of many reasons data encryption is considered a best practice and sound investment for IT security.

A Ponemon Institute study, *Patient Privacy & Data Security* found that the average economic impact of a data breach has increased by $400,000 to a total of $2.3 million since 2010.[3]

[2] Dept. of Health & Human Services; *Breach Notification for Unsecured Protected Health Information* (PDF)

[3] The Ponemon Institute; *Third Annual Benchmark Study on Patient Privacy & Data Security* (PDF)

Figure 3. Economic impact of data breach incidents experienced over the past two years



Source: The Ponemon Institute, Patient Privacy & Data Security

The economic impact can include investigation and legal fees, federal penalty costs, business loss due to downtime, decreased credibility and remediation or free credit monitoring for affected individuals. Costs will only continue to increase as the healthcare industry increases their reliance on electronic medical record systems (EMRs) and electronic health records (EHRs).

Unsecured, or unencrypted data, is a reoccurring and common theme in healthcare data breaches. Take these data breach cases, for example, that all involve unencrypted data and devices:

- The Alaska Medicaid program was fined $1.7 million after a breach resulting from an unencrypted USB device that contained just 501 patient records was stolen.[4]
- Massachusetts Eye and Ear Associates was fined $1.5 million after a breach resulting from the theft of an unencrypted laptop containing about 3,600 of its patients and research subjects.[5]
- Advocate Health Care lost four million patient records when four unencrypted computers were stolen from their facility; the second largest health data breach since 2009.[6]

[4] Health Data Management; OCR Fines Alaska Medicaid $1.7 Million for HIPAA Violations
[5] Dept. of Health & Human Services; Massachusetts Provider Settles HIPAA Case for $1.5 Million

- TRICARE Management had unencrypted backup tapes stolen, affecting 4.9 million individuals; the largest health data breach to date.[7]

Only unencrypted data falls under the scope of the HIPAA Breach Notification Rule that requires patient, media and Dept. of Health and Human Services notification. Meaning, if you encrypt your data, you do not have to report a data breach to the government unless you have reason to believe that the encryption keys were compromised.

While encryption is "addressable" under HIPAA, it is highly recommended. OCR (Office for Civil Rights) Director Leon Rodriguez was quoted: "…Encryption is an easy method for making lost information unusable, unreadable and undecipherable." We will not debate if encryption is "easy" in this white paper, but it is key to recognize that the Department of Health and Human Services, who enforces HIPAA violation investigation and penalties through its Office for Civil Rights considers encryption well within reach with the burden of proof on the organization that chooses not to implement it.

The HIPAA Security Rule for healthcare organizations handling electronic protected health information (ePHI) dictates that organizations must:

> *In accordance with §164.306… Implement a mechanism to encrypt and decrypt electronic protected health information. (45 CFR § 164.312(a)(2)(iv))*

HIPAA also mandates that organizations must:

> *§164.306(e)(2)(ii): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. Protecting ePHI at rest and in transit means encrypting not only data collected or processed, but also data stored or archived as backups.*

HIPAA Encryption of Data at Rest

The HIPAA Breach Notification Rule[8] provides guidance on encryption, stating that the proper standards for encrypting data at rest are aligned with the NIST (National Institute of Standards and Technology) Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.[9] The NIST standard approves of the AES algorithm (Advanced Encryption Standard).

Data at rest can include database fileshares, workstations, laptops, tablets, iPads, phones, USB drives, flash drives, data backup tapes, CDs and DVDs, cameras and external hard drives.[10]

[6] Chicago Tribune Business; Regulators to Investigate Advocate Health Data Breach
[7] Modern Health Care; Breach Spurs Lawsuit Seeking $4.9 Billion
[8] U.S. Dept. of Health & Human Services; Breach Notification Rule
[9] National Institute of Standards and Technology (NIST); Guide to Storage Encryption Technologies for End User Devices (PDF)
[10] Chris Heuman, CISSP, CSCS, CHP; Encryption: Perspective on Privacy, Security & Compliance webinar/slides (PDF)

The SANS Institute, specializing in Internet security training, recommends employing whole-disk or folder-level encryption for ePHI. For ePHI in databases, they recommend full database or column-level encryption. Additionally, key management procedures and processes that separate duties and least-privilege for users and applications are important for ePHI at rest. Lastly, they recommend hashing or digitally signing all stored ePHI.[11]

HIPAA Encryption of Data in Transit

For data in transit (also referred to as “in flight”), complying with the Federal Information Processing Standards (FIPS) 140-2 also includes standards described in NIST Special Publication 800-52, 800-77 and 800-113.[12] Data in transit crosses the Internet, wireless networks, from tier to tier within an application, or across wired or wireless connections without being stored. Data in transit remains in a non-persistent state - where it's not being written to disk or other media or being retained.

The SANS Institute recommends implementing a VPN (Virtual Private Network) using either IPSec or SSL for all remote systems that need to transmit ePHI, and to implement encryption for all systems and users that may need to email ePHI. Many organizations add two-factor authentication to their VPN login process such as Duo Security to further protect data and prevent unauthorized use.

HIPAA Encryption in the Cloud and Data Center

Encrypting data at rest and in transit is key to protecting ePHI. Encryption should be addressed both in transit through SSL connections or VPN tunnels as well as at the disk level. If IT infrastructure is outsourced, make sure to read the details of their audit reports and that the hosting provider will sign a Business Associate Agreement (BAA).

Reviewing the hosting provider’s data breach insurance policy can also be a key indicator of the level of attention and priority given to preventing data breaches. HIPAA compliant data centers should be able to turn over a complete HIPAA risk assessment performance against the OCR HIPAA Audit protocol guidelines or equivalent documentation of controls that prove thorough due diligence to protect sensitive data.

Particularly in the cloud, encryption is an important aspect of keeping data safe and in compliance with the HIPAA Security Rule. A HIPAA compliant cloud should provide encryption of data at rest, including data that is stored as backups and archived as part of an IT disaster recovery plan. The cloud should also provide encryption of data in transit for complete security.

Read our **HIPAA Compliant Hosting White Paper** for details on achieving compliance with health IT, including a diagram of a HIPAA compliant infrastructure, and what to look for in a HIPAA hosting provider.

[11] The SANS Institute; *Regulations and Standards: Where Encryption Applies* (PDF)
[12] U.S. Dept. of Commerce; *FIPS Publication: Security Requirements for Cryptographic Modules* (PDF)

2.2. PCI DSS Encryption

The PCI DSS (Payment Card Industry Data Security Standard) requires companies that deal with credit cardholder data to employ encryption or other technology to render data unreadable:

> *3.4 Render PAN (Primary Account Number) unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:*
>
> - *One-way hashes based on strong cryptography (hash must be of the entire PAN)*
> - *Truncation (hashing cannot be used to replace the truncated segment of PAN)*
> - *Index tokens and pads (pads must be securely stored)*
> - *Strong cryptography with associated key-management processes and procedures*
>
> *3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored.*

When it comes to data storage, the PCI Security Standards Council (SSC) recommends that merchants render cardholder data unreadable by using strong cryptography, and to use other layered security technologies to minimize risk of criminal exploits. They also warn against locating servers or other payment card system storage devices outside of a locked, fully-secured and access-controlled room.[13]

One way to achieve this is by partnering with a PCI hosting provider that can meet the physical and technical requirements of the standard by maintaining a PCI compliant data center. Physical security should include locked server racks, suites and cages, and dual-identification control access to data centers. Environmental control can be achieved with 24x7 monitoring, logged surveillance and alarm systems.

The PCI SSC specifically recommends ‘strong cryptography’ which they define as cryptography that is based on industry-tested and accepted algorithms, key lengths and proper key management practices. They call out AES (128 bits and higher) as an example of strong cryptography[14] and refer technical users to the NIST Special Publication 800-57 (three parts) on recommendations for key management.[15]

P2PE (Point-to-Point Encryption)

Merchants that transmit cardholder data from a POS terminal (Point of Sale) to a payment processor should use point-to-point encryption (P2PE) to secure data and reduce risk of unauthorized interception during transmission. While the PCI SSC released a very detailed document outlining infrastructure encryption requirements, a high-level overview of the six main areas that must be secured within the SCD (secure cryptographic devices, or the hardware/hardware level) include:

[13] PCI Security Standards Council; *PCI Data Storage Do’s and Don’ts* (PDF)
[14] PCI Security Standards Council; *Glossary of Terms, Abbreviations and Acronyms* (PDF)
[15] National Institute of Standards and Technology (NIST); *SP 800-57 Part 1-3*

1. **Encryption Device Management**: Use secure encryption devices and protect devices from tampering. Requirements include building/using PCI-approved POI devices (Point of Interaction, or the device that accepts PINs), and securely managing equipment used to encrypt account data. The POI device should be managed by the solution provider and hardware encryption should be performed by the device.
2. **Application Security**: Secure applications in the P2PE environment. Requirements include protecting PAN/SAD (Primary Account Number and Sensitive Authentication Data); developing and maintaining secure apps; and implementing secure app-management processes. Apps should be on PCI-approved POI devices.
3. **Encryption Environment:** Secure environments where POI devices are present. Requirements include not storing CHD after transactions are complete, securing POI devices throughout their lifecycle, implementing secure device management processes and maintaining a *P2PE Instruction Manual* (PIM) for merchants.
4. **Segmentation between Encryption and Decryption Environments:** Segregate duties/functions between encryption and decryption environments. Requirements include all decryption operations managed by solution provider; merchant has no access to the encryption or encryption environment and the merchant has no involvement in the operations.
5. **Decryption Environment and Device Management:** Secure decryption environments/devices. Requirements include using only approved decryption devices; securing all decryption systems and devices; implementing secure device-management processes and maintaining secure decryption environment. The merchant must also have no access to the decryption environment and the decryption environment must be PCI DSS compliant.
6. **Cryptographic Key Operations:** Use strong cryptographic keys and secure key management functions. Requirements include using secure encryption and key generation methods; and distribute, load, use and administrate cryptographic keys in a secure manner.

See the *PCI Point-to-Point Encryption: Solution Requirements and Testing Procedures v1.1.1 Encryption, Decryption and Key Management within SCDs (Hardware/Hardware)* document for more details and testing procedures to help you build and verify a valid P2PE solution that meets the PCI SSC standards for hardware encryption.[16]

Read our **PCI DSS Compliant Hosting White Paper** for details on what a PCI DSS compliant IT infrastructure should entail, including technical services that can help fulfill the requirements of the standard for the ecommerce and retail industry.

[16] PCI Security Standards Council; *PCI Point-to-Point Encryption: Solution Requirements and Testing Procedures v1.1.1 Encryption, Decryption and Key Management within SCDs (Hardware/Hardware)* (PDF)

2.3. SOX Encryption

SOX, or Sarbanes-Oxley Act, was created to protect the sensitive financial reporting data in public companies. While not explicitly stated, encryption can help satisfy the requirements as follows:

> *DS5.11 Exchange of Sensitive Data: Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt, and non-repudiation of origin.*
>
> *DS11.6 Security Requirements for Data Management: Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, organizational security policy, and regulatory requirements.*
>
> *DS5.8 Cryptographic Key Management: Determine that policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.*

The SANS Institute recommends more general encryption best practices, such as employing remote management using secure encrypted channels (SSH, SSL, and IPSec); encrypting security device log data at rest and in transit; using dedicated key storage devices and apps; role-based key access policies; key recovery procedures, and guidance of key handling in different environments.[17]

[17] The SANS Institute; Regulations and Standards: Where Encryption Applies (PDF)

3.0. Encryption Guidelines

3.1. Find, Classify and Determine What to Encrypt

Determining what kind of data to encrypt is the first objective to protecting it. Your organization needs to determine where your data is located, how sensitive it is and what is in your data repositories in order to protect it with encryption.

Classifying your data as **regulated**, or data that falls under the data protection laws such as HIPAA or PCI, can clarify what you should encrypt. A few examples of regulated data include personally identifiable data, patient data or credit cardholder data. It can be inefficient to attempt to encrypt everything – finding the sensitive data that is transmitted as network traffic, found in file shares, databases and all endpoints helps you specify where it is necessary to employ encryption.

Non-centralized and unstructured repositories such as Word documents, spreadsheets and text files are also at risk to be overlooked and unsecured. A recent healthcare data breach by the Oregon Health & Science University (OHSU) was a result of several health departments using unencrypted Google spreadsheets to maintain and exchange patient information.[18] Data sharing outside of the centralized database can lead to unsecure practices.

Confidential data is another category your data may fall under – this might include client contracts, purchasing agreements, etc. While a breach of this type of data may not get you fined by federal law or regulatory entities, your organization likely does not want these documents available to the public. **Non-public** data may be employee-related, such as salary history, payroll, leave, etc. And **public** information is data available on your website, such as marketing materials that are intended to be distributed publicly.

After classifying your data, you should be able to make an encryption determination about which categories of data you want to encrypt. Creating an asset inventory that correlates classified data to certain devices, disks, storage area networks and servers is next as you consider where you should employ encryption.

3.2. Encryption Guidelines

3.2.1. Data at Rest

Data at rest, or in storage, may include end user devices such as personal computers, mobile devices and removable storage media. Encryption for stored data can be applied to one individual file with sensitive data or applied to all stored data, as previously mentioned.

[18] Online Tech; *No Encryption or BAAs: Keep PHI off Unsecure Clouds*

NIST explains some of the high-level security controls required for secure and encrypted stored data:

Authentication
Encrypted stored data requires users to verify their identity and authenticate to gain access by means of an authentication method; including passwords, personal ID numbers (PINs), biometrics, tokens, etc.

Data Backups
While storing backups at an offsite location is good practice for organizations in case of a disaster, they must also be encrypted and secured. Traditional tape backup puts you at risk of physical loss of data. Using a cloud-based disaster recovery solution eliminates tape backup and virtualizes the entire operation system, apps, patches and data.

Encrypting sensitive data before it is sent to an offsite backup facility is another way to ensure data is secure. NIST recommends any local backups should also be encrypted and physically secured within the organization's facilities.

End User Devices
Securing and maintaining device operating systems, apps and wired or wireless network traffic should also help reduce the risk of a data breach.

See section *5.0. Choosing Encryption Techniques* for a more technical overview of encrypting data at rest.

3.2.2. Data in Transit

Although encryption of data at rest is mainly the focus for security since it is more likely that a hacker will target systems with data on local drives or storage networks, encrypting data in transit is also important to avoid potential interception by unauthorized persons. Data in transit may include data that travels across the Internet, wireless networks, from tier to tier within an application, across wired or wireless connections in a non-persistent state.

Complying with the Federal Information Processing Standards (FIPS) 140-2 that includes the standards described in NIST SP 800-52, -77 and -113 can provide acceptable encryption for data in transit for the healthcare industry, which can also work for other industries.[19]

Virtual Private Network (VPN)
When using a VPN (Virtual Private Network), you are connecting one network to another network in order to access a server remotely – this means you are also transmitting data that needs to be encrypted. VPNs can use a variety of secure protocols to transmit, or tunnel traffic

[19] National Institute of Standards and Technology; *Security Requirements for Cryptographic Modules* (PDF)

from one network to another securely. The data is encrypted while sent from one network to another, and the VPN server decrypts the data and forwards it to the receiving server.

Two-Factor Authentication

Two-factor authentication for VPN (Virtual Private Network) access is an optimal security measure to protect against online fraud and unauthorized access for clients that connect to their networks from a remote location.

Two-factor authentication (also known as dual-factor or multi-factor) requires the use of one form of authorization (username/password), and an additional form of authentication to gain access to a network remotely. Two-factor authentication provides an extra layer of protection to ensure the user is truly the one who is allowed access to the network, and to protect against unauthorized entry.

SSL Certificates

SSL (Secure Sockets Layer) is a cryptographic protocol that can provide security as information is transmitted over the Internet. When a browser tries to connect with a website secured with SSL, the browser first requests that the web server identify itself. After the server sends a copy of its SSL certificate, the browser checks its credentials and approves it. The server then sends a digital signature to start an encrypted SSL session, and then encrypted data is shared between the browser and server.[20]

SFTP

Another method for securing data in transit is with SFTP, the SSH File Transfer Protocol that allows for secure file transfers between hosts as well as access/management of files on remote file systems. SFTP ensures that the data being transmitted is secured as well as your login credentials.

To create a strong layered security solution, use both a VPN and SSL connection. A VPN can transmit data securely even for standards that don’t have encryption built in. While the file itself isn’t encrypted, the entire path that the file traverses is encrypted.

[20] Symantec; *Secure Sockets Layer (SSL): How It Works*

4.0. Choosing Encryption Techniques

4.1. Storage-Level Encryption

4.1.1. Full Disk Encryption (FDE) or Whole Disk Encryption (WDE)

Full disk encryption (FDE) is the encryption of all data on a hard drive used to boot a computer. NIST explains software-based FDE to function as the following:

When FDE software is installed on a computer, the computer's master boot record (MBR – that which determines which software will be executed when the computer boots from the media) redirects from the computer's primary operating system to a pre-boot environment (PBE). This PBE controls access to a computer and requires some type of authentication (username/password) before decrypting and booting the OS.

NIST notes that there may be a marginal delay in opening or saving files as the FDE software transparently decrypts and encrypts the parts of the hard drive as needed. FDE software can also cause conflicts with other software at the disk level that also store code in the same space as the PBE.

For the hardware solution, FDE can be built into a hard drive disk controller. Hardware-based FDE cannot be disabled or removed from the drive – the encryption code and authenticators, including passwords and keys, are also stored on the hard drive. According to NIST, since there is no OS role in encryption/decryption, there is typically very little performance impact.[21]

Additionally, software-based FDE can be centrally managed, but hardware-based FDE can typically be only managed locally, which can make key management more resource-intensive for hardware-based FDE.

Database encryption also doesn't protect against application-level attacks since the encryption function is implemented within the database management system (DBMS).[22]

Windows Disk Encryption

For Microsoft disk encryption, EFS (Encrypting File System) is a feature of Windows that uses AES to encrypt data at rest. Another service available for Windows Server 2008 and up is Windows Bitlocker that allows you to encrypt your hard drives. Bitlocker uses 128 or 256-bit AES encryption, which is recommended by NIST. Integrating BitLocker helps guard against data theft or exposure in the case of a lost or stolen decommissioned computer.[23] As part of the operating system install, BitLocker is not enabled until it's initialized by using the setup wizard.

[21] National Institute of Standards and Technology (NIST); *Guide to Storage Encryption Technologies for End User Devices* (PDF)

[22] Protegrity Corp., *Database Encryption – How to Balance Security with Performance* (PDF)

[23] Microsoft TechNet Library; *BitLocker Drive Encryption Overview*

Linux Disk Encryption
For Linux disk encryption, LUKS (Linux Unified Key Setup) is a platform that can integrate with Windows using FreeOTFE. LUKS uses dm-crypt, which is a disk encryption system within the kernel. The advantage of LUKS is that you can encrypt individual partitions, such as the partition on which the data lives. In the event the system was stolen, and the hard drive was swapped out, the data would still be secure.

4.1.2. Virtual Disk/Volume Encryption

With virtual disk encryption, a container that holds many files and folders is encrypted. After authentication, the container is then typically mounted as a virtual disk. The container is a single file within a logical volume; one example is the boot, system and data volumes on a personal computer.

Volume encryption is the process of encrypting an entire logical volume. Examples include volume-based removable media like USB flash drives and external hard drives.

4.1.3. File/Folder Encryption

Individual files are encrypted on a storage medium, and the same with folder encryption. The difference between virtual disk/volume and file/folder encryption is that a container is completely encrypted and no data can be viewed until after decryption. File/folder encryption allows anyone with access to the file system to read titles and other metadata for the encrypted files and folders. According to NIST, common options for customizing file/folder encryption include:

- Allowing the user to designate which files and folders should be encrypted
- Automatically encrypting:
    - Administrator-designated folders
    - Certain file types, denoted by a particular file extension (i.e., .doc or .png)
    - All files written by particular applications
    - All data files for certain users

4.2. Database-Level Encryption

Database-level encryption is the process of encrypting data as it is written to and read from a database. This level of encryption can protect against storage media theft and database-level attacks, but it does not encrypt data transmitted over networks.

Typically, database-level encryption is done at the column-level within a database table; as an alternative to whole database encryption, column encryption encrypts individual columns of data. Column-level encryption can hide data in each cell or data field in a particular column from certain user groups that don’t have access to the entire data table.

Column-level encryption allows you to protect columns in databases that exist in different platforms. Other methods of database encryption include more granular approaches, from row, cell, table space and file-level encryption that require authentication for each.

Encrypting the entire database is easy and faster to implement than encrypting select data, however, it is very resource-intensive. It may work well for a small-sized database but it could slow down a large database due to increased demands on system resources. In SQL Server 2008, when the entire database is encrypted, the entire database needs to be decrypted before you can access or query the database.

4.3. Application-Level Encryption

Encrypting data at the application-level allows for more granular and custom encryption of data, meaning the application can identify where and what sensitive data to encrypt, and has insight into which users have what kind of access.

How does it work? A user connects to their company's system via a VPN and then sends data to an SSL protected website. After they upload their files, they are encrypted on the system servers. The application server decrypts the contents of the files and determines how to store the data in the database.

Application-level encryption is still at risk for hackers that may use development tools to gain access to encryption keys to decrypt or turn off encryption and gain access to data within the application. Application-level encryption also does not protect against database attacks. Encryption at the application layer can also affect performance of the application, particularly applications that need to process large volumes of data at a fast rate.

5.0. Keys

Cryptographic keys are essential to data encryption security, as your data security is only as strong as your key management. Keys need to be protected against modification and unauthorized disclosure, as well as preserved for the entire lifetime of the data. NIST defines the different types of cryptographic keys as the following:

1. **Public Signature Key –** This is one of the keys in the key pair used by an asymmetric (public) algorithm to verify digital signatures.
2. **Private Signature Key –** The other key in the key pair used by an asymmetric (public) algorithm to generate digital signatures.
3. **Public Authentication Key –** Used in an asymmetric (public) key pair, the public authentication key provides assurance of the identity of the originating entity.
4. **Private Authentication Key –** Used in an asymmetric (public) key pair, the private authentication key provides assurance of the identity of the originating entity.
5. **Symmetric Authentication Key –** Used with symmetric key algorithms to provide source authentication and protect data integrity.

For a full list of the different types of keys, refer to the NIST Special Publication 800-57, *Recommendation for Key Management: Part 1: General (Revision 3)*.[24]

From a high-level overview, key management, including policies and procedures for key use are very important for encryption effectiveness. Some of the basic key policies that should be addressed by your organization are:[25]

- How are keys stored? For Full or Whole Disk Encryption, cryptographic keys are stored securely on the hard drive
- Ensure unique keys are provided by technology vendors – often the same keys are used across multiple organizations, which can present a major risk
- Different keys should be generated for different cryptographic systems and different applications
- Key distribution and how keys should be activated when received
- Key storage, as well as how authorized users obtain access to the keys
- Changing or updating keys, and rules on when keys should be changed
- Dealing with keys that have been compromised – either accessed by unauthorized users or manipulated in any way
- Key recovery in the event that keys are lost or corrupted, as part of your business continuity and IT disaster recovery plan
- Archiving, destroying, logging of keys and key management activities

For secure key management systems, the following precautions and best practices should be followed:

- Fully automated key management – cutting down on potential key exposure by personnel
- No key should appear unencrypted
- Keys should be randomly chosen from the entire key space and preferably by hardware
- Key-encrypting keys are separate from data keys, and no data ever appears in plaintext that was encrypted using a key-encrypting key. (A key-encrypting key is used to encrypt other keys, securing them from disclosure)
- Keys with a long life should be rarely used, as the more a key is used, the greater the opportunity for a hacker to discover the key
- Keys should be changed frequently to increase the effective key length of an algorithm
- Keys transmitted should be sent securely to authenticated users
- Key generating equipment should be physically and logically secure during installation, operation and removal from service

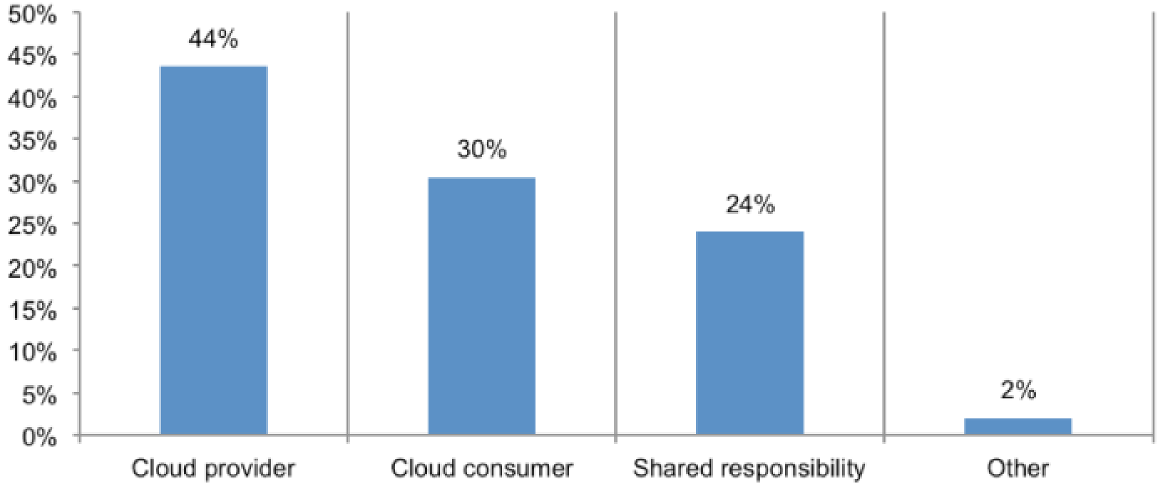
[24] NIST; Special Publication 800-57, *Recommendation for Key Management: Part 1: General (Revision 3)* (PDF)

[25] Chris Heuman CHP, CHSS, CSCS, CISSP, Practice Leader, RISC Management & Consulting; *Encryption – Perspective on Privacy, Security & Compliance* (Webinar)

6.0. Encryption in the Cloud

According to a Ponemon Institute study on *Encryption in the Cloud*, about half of the respondents transfer sensitive or confidential data to a cloud environment, including regulated data that falls under compliance laws.[26] Yet, when it comes to security responsibilities, 44 percent believe the cloud provider has primary responsibility for protecting sensitive or confidential data in the cloud environment, while 30 percent believe it is up to the cloud consumer.

Figure 3. Who is most responsible for protecting data in the cloud?
Consolidated view



Source: The Ponemon Institute, Encryption in the Cloud

As the Center for Democracy and Technology stated in a FAQ on HIPAA and cloud computing:

> *Cloud computing outsources technical infrastructure to another entity that essentially focuses all its time on maintaining software, platforms or infrastructure. But a covered entity such as a health care provider still remains responsible for protecting PHI in accordance with the HIPAA Privacy and Security Rules, even in circumstances where the entity has outsourced the performance of core PHI functions.*[27]

Point being, data security in the cloud is still the responsibility of both the organization and its cloud service provider, and for certain compliance standards, the organization is held liable in the case of a data breach.

However, gaining transparency into your cloud provider's environment can help you determine how secure your sensitive data will be in your cloud infrastructure. While some providers do not provide built-in encryption, others may provide both encryption of data at rest (in storage) and

[26] Ponemon Institute, Encryption in the Cloud
[27] Center for Democracy and Technology (CDT), FAQ: HIPAA and "Cloud Computing" (v1.0)

data in transit so you don't have to seek another vendor for a software-based cloud encryption solution for the complete data security package.

6.1. Outsourcing the Encrypted Cloud

This paper will discuss outsourcing the cloud model infrastructure as a service (IaaS) in which a cloud service provider supplies the hardware, networking and maintenance, while the application is managed by the organization. As the CDT stated, the outsourced cloud is beneficial for many reasons:

- The cloud offers faster computing performance, capacity, flexibility and security at lower costs.
- Cloud providers allow organizations to focus resources on their core business, not IT.
- For companies with limited IT staff and budget, outsourcing allows them to take advantage of a cloud provider's investments in software and hardware upgrades.
- For companies that require storage and resource-intensive support (i.e. medical imaging documents and applications), the cloud can quickly scale to meet unexpected demands.
- An encrypted cloud offers protection of data in transit and at rest – depending on the technology used; it can provide security without affecting performance.

6.2. Considerations

What should you look for if you plan to outsource your cloud infrastructure to an encrypted cloud hosting provider? For complete assurance of your data's security in the cloud, check for the following:

1. **Encryption.** Ask if they offer encryption of data at rest and in transit, and how it is implemented to avoid spending to add software-based encryption that may slow your cloud down.
2. **Audit Reports on Compliance.** For general assurance of a cloud provider's data center facility security, check for a SSAE 16 or SOC 2 report (see the *section 8.1 Data Center Audits Cheat Sheet* for details). For industry-specific compliance, check for a HIPAA or PCI DSS Report on Compliance (ROC), as well as the dates of their last audit.
3. **Policies and Procedures.** Ask about your cloud provider's policies and procedures around data breach notification, data access, technical services for compliance, data termination after contract end and more.
4. **Private Clouds.** With a private cloud, you can ensure your resources are dedicated to only your organization and always available for you when you need them. Some public clouds allocate resources to other tenants on a first-come, first-served basis.
5. **Disaster Recovery and Offsite Backup.** For compliance and best practice, establishing a backup and complete disaster recovery (DR) plan can help recover systems in the event of a natural disaster or other unforeseen business disruption. Ask your cloud provider what kind of DR and backup services they can integrate with your service.

Our Encrypted Cloud Solution

Online Tech's cloud encrypts data at rest and in transit at the drive-level within a storage area network (SAN) provided by EMC, called the VMAX SAN. Our enterprise-class clouds are an example of how hardware-based encryption can provide data security and meet compliance requirements while having no impact on cloud performance.

Using built-in, hardware-based data encryption, the data is encrypted when written to drives and decrypted when read from drives. This type of back-end encryption ensures there is no risk of stored data exposure when drives are removed or arrays are replaced.[28]

For key management, EMC uses their RSA Embedded Key Manager that provides self-managed, separate and unique DEKs (data encryption keys) for each drive in the array. The RSA key manager follow the key generation, distribution and management capabilities as defined by the industry standards NIST 800-57 and ISO 11770. Audit logs keep track of key management activities; including key creation, key deletion and key recovery.

Their keys are kept in a 'key lockbox' – a repository encrypted with 256-bit AES. For more about their secure key management and data encryption; including detailed examples of how data stays encrypted during installation, drive replacement and system decommissioning; read their white paper, *EMC Symmetrix Data at Rest Encryption: Detailed Review* (PDF).

When paired with the use of VPNs (Virtual Private Networks), SSL certificates and two-factor authentication for VPN by the client when connecting with a mobile device remotely, the data is transferred encrypted and then stored in the VMAX SAN, encrypted. This can create a completely encrypted environment for data to be shared and stored safely within compliance requirements.

Ensure reliability of data in transit in the cloud with high availability (HA), dedicated firewalls, web application firewalls and servers. High availability solutions in the data center infrastructure allow organizations to increase their uptime and availability. When mission-critical data is at stake, using an HA architecture can greatly reduce the risk of downtime to your business due to a single point of failure. With HA protection in place, businesses can hedge against the loss of electrical power and network connectivity disruptions, and have the peace of mind in knowing your data is protected, available, and safe.

Data center infrastructure components should be designed to ensure no single points of failure exist for a successful cloud implementation. Those components include:

- Electrical power connections
- UPS (Uninterruptible Power Supply) systems
- Generators
- Air conditioning
- Network connections, switches and firewalls

[28] EMC Corporation; *EMC Symmetrix Data at Rest Encryption: Detailed Review* (PDF)

- Server and storage devices

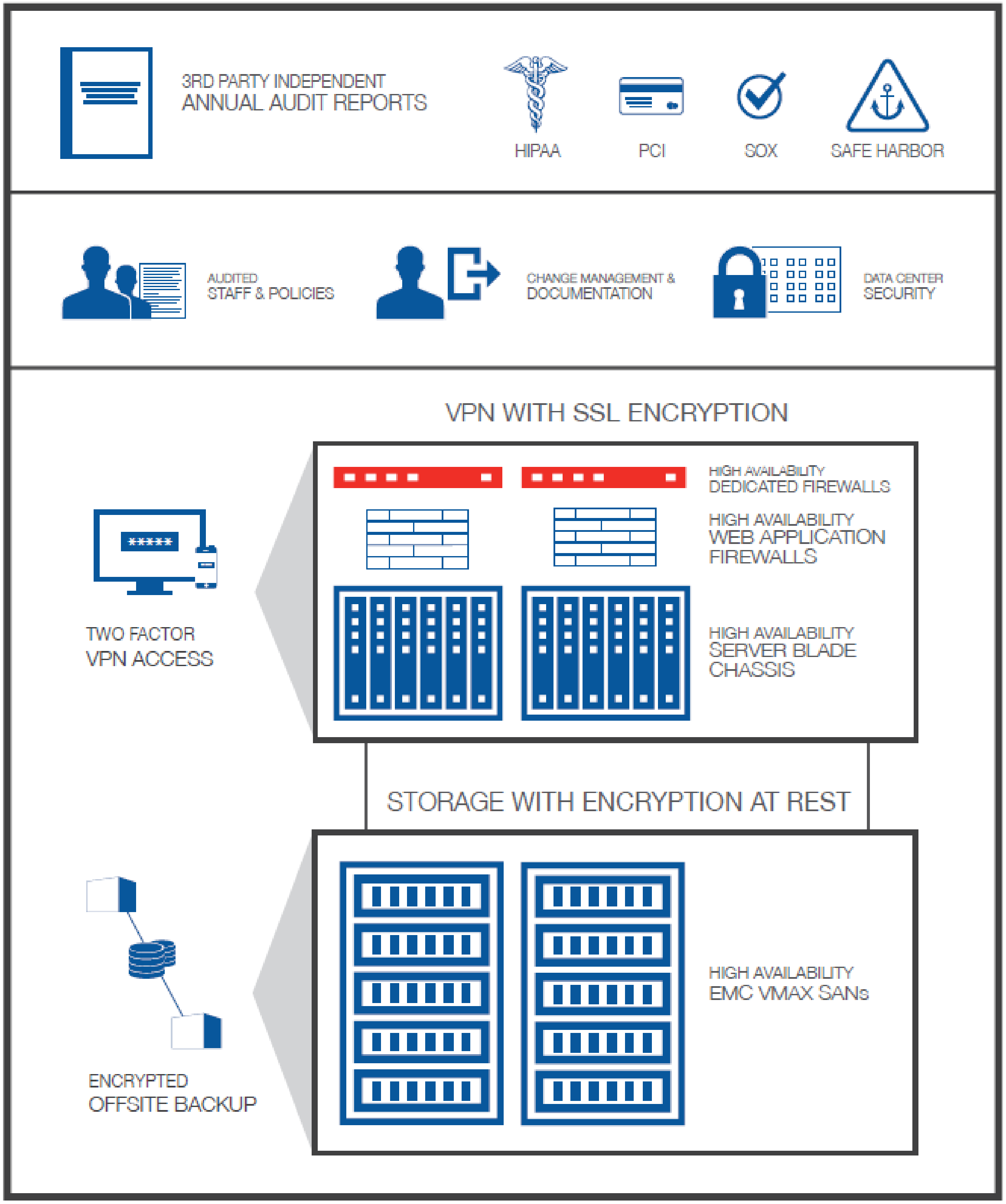
Read more about Online Tech’s Encrypted Cloud (PDF).

Online Tech’s Defense-in-Depth Stack

The following diagram shows each component of a solid defense-in-depth, encrypted hosting solution, including:

- Industry-specific audit reports
- Administrative safeguards, including change management and documentation; and audited staff and policies
- Encryption of data in transit with VPN, SSL, two-factor authentication for VPN and high availability, redundant critical hardware
- Encryption of data at rest with high availability EMC VMAX SANs and encrypted offsite backup

DEFENSE IN DEPTH



Additional Technical Security Tools

As mentioned before, encryption is but one tool that can be used in conjunction with other technical security tools to ensure a layered, defense-in-depth IT security solution. Find out more about each tool and how they work to protect your systems, networks, servers and data:

Daily Log Review

Some providers may only offer logging (tracking user activity, transporting and storing log events) - seek a provider that offers the complete logging experience with daily log review, analysis, and monthly reporting.

File Integrity Monitoring (FIM)

Monitoring your files and systems provides valuable insight into your technical environment and provides an additional layer of data security. File integrity monitoring (FIM) is a service that can monitor any changes made to your files.

Web Application Firewall (WAF)

Protect your web servers and databases from malicious online attacks by investing in a web application firewall (WAF). A network firewall's open port allows Internet traffic to access your websites, but it can also open up servers to potential application attacks (database commands to delete or extract data are sent through a web application to the backend database) and other malicious attacks.

Two-Factor Authentication

Two-factor authentication for VPN (Virtual Private Network) access is an optimal security measure to protect against online fraud and unauthorized access for clients that connect to their networks from a remote location.

Vulnerability Scanning

Vulnerability scanning checks your firewalls and networks for open ports. It is a web application that can detect outdated versions of software, web applications that aren't securely coded, or misconfigured networks. If you need to meet PCI compliance, you need to run vulnerability scans and produce a report quarterly.

Patch Management

Why is patch management so important? If your servers aren't updated and managed properly, your data and applications are left vulnerable to hackers, identity thieves and other malicious attacks against your systems.

	Antivirus Antivirus software can detect and remove malware in order to protect your data from malicious attacks. Significantly reduce your risks of data theft or unauthorized access by investing in a simple and effective solution for optimal server protection.
	SSL Certificate In order to safely transmit information online, a SSL (Secure Sockets Layer) certificate provides the encryption of sensitive data, including financial and healthcare. A SSL certificate verifies the identity of a website, allowing web browsers to display a secure website.

7.0. Conclusion

Encryption is a key technical tool within a comprehensive security strategy designed to protect sensitive data that may be regulated by compliance standards such as HIPAA or PCI DSS. Determining the best method to use for your organization is a start to implementing encryption within the broader security framework of your infrastructure.

For data at rest, including stored, archived and data found on electronic devices, hardware-based encryption at the disk-level can provide seamless data protection without affecting the performance of the cloud. For data in transit, including data traveling across the Internet, wireless networks, within an application, or across wired or wireless connections, a combination of SSL certificates, VPN (Virtual Private Networks) and two-factor authentication can ensure data is encrypted at all times along its path.

When outsourcing the cloud, look for built-in encryption options, audit reports, additional technical security services to accompany encryption, disaster recovery and offsite backup options, and robust encryption key management. Remember, your encryption method is only as strong as your key management, and the ability to keep keys secure.

8.0. References

8.1. Encryption Glossary

AES (Advanced Encryption Standard)
The Advanced Encryption Standard specifies a federally-approved algorithm used to protect electronic data, considered strong enough to satisfy Federal Information Processing standards (FIPS). The algorithm encrypts and decrypts information, and is capable of using cryptographic keys of 128, 192 and 256 bits.

Asymmetric Key Cryptography (Public-Key Cryptography)

Encryption in which one key is used to encrypt messages (public key), while a private key is used to decrypt them. The private key must be kept secret, while the public key has no risk even if it becomes known to others (the public key is meant to be shared).

Cryptography

Storage encryption technology uses cryptographic keys to encrypt and decrypt data. Cryptography is based on computationally secure algorithms designed to protect data.

Cryptographic Hash

This is the algorithm that can change a large block of data into a fixed-length string; the cryptographic hash. No two blocks of different data have the same hash. This is an example of one-way encryption. A hacker who obtains the password cannot run the hash through an algorithm to decrypt the password.

Ciphertext

After plaintext has been passed through a cryptographic encryption algorithm, ciphertext is the result. Ciphertext is irreversible without the encryption key.

Data Encryption Key (DEK)

Used for the encryption of plaintext and for the computation of message integrity checks (signatures).

Encryption

Rendering plaintext into ciphertext, meaning to render original data unreadable or undecipherable.

File Encryption

Individual files are encrypted on a storage medium and are accessible only after proper authentication.

Full Disk Encryption (FDE)

All of the data on the hard drive used to boot a computer, including the computer's operating system, is encrypted.

Key Size

The key size/length is measured in bits of the key used in a cryptographic algorithm – for AES; there is a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

Symmetric Key Cryptography

Encryption in which the sender/receiver of a message shares a single key used to both encrypt/decrypt the message. Symmetric encryption relies on the secrecy of the key.

Volume Encryption

An entire volume is encrypted and access to the data on the volume is allowed only after authentication.

8.2. Data Center Audits Cheat Sheet

SAS 70

The Statement on Auditing Standard No. 70 was the original audit to measure a data center's financial reporting and recordkeeping controls. Developed by the AICPA (American Institute of CPAs, there two types:

- **Type 1 –** Reports on a company's description of their operational controls
- **Type 2 –** Reports on an auditor's opinion on how effective these controls are over a specified period of time (six months)

SSAE 16

The Statement on Standards for Attestation Engagements No. 16 replaced SAS 70 in June 2011. A SSAE 16 audit measures the controls relevant to financial reporting.

- **Type 1** – A data center's description and assertion of controls, as reported by the company.
- **Type 2 –** Auditors test the accuracy of the controls and the implementation and effectiveness of controls over a specified period of time.

SOC 1

The first of three new Service Organization Controls reports developed by the AICPA, this report measures the controls of a data center as relevant to financial reporting. It is essentially the same as a SSAE 16 audit.

SOC 2

This report and audit is completely different from the previous. SOC 2 measures controls specifically related to IT and data center service providers. The five controls are security, availability, processing integrity (ensuring system accuracy, completion and authorization), confidentiality and privacy. There are two types:

- **Type 1** – A data center's system and suitability of its design of controls, as reported by the company.
- **Type 2** – Includes everything in Type 1, with the addition of verification of an auditor's opinion on the operating effectiveness of the controls.

SOC 3

This report includes the auditor's opinion of SOC 2 components with an additional seal of approval to be used on websites and other documents. The report is less detailed and technical than a SOC 2 report.

HIPAA

Mandated by the U.S. Health and Human Services Dept., the Health Insurance Portability and Accountability Act of 1996 specifies laws to secure protected health information (PHI), or patient health data (medical records). When it comes to data centers, a hosting provider needs to meet HIPAA compliance in order to ensure sensitive patient information is protected.

A HIPAA audit using the testing guidelines provided by the OCR HIPAA Audit Protocol can provide a documented report to prove a data center operator has the proper policies and procedures in place to provide HIPAA hosting solutions.

PCI DSS
The Payment Card Industry Data Security Standard was created by the major credit card issuers, and applies to companies that accept, store process and transmit credit cardholder data. When it comes to data center operators, they should prove they have a PCI compliant environment with an independent audit. They should also know what services can help your company fulfill the 12 PCI requirements.

9.0. Contact Us

Contact our encrypted cloud and hosting experts at Online Tech for more information if you still have questions about secure and compliant hosting at our data centers.

Visit: www.onlinetech.com
Email: contactus@onlinetech.com
Call: 734.213.2020