

HIPAA Security Rule Compliance with Server General



The HIPAA Security Rule requires health care organizations (covered entities and their business associates) to secure the protected health information (PHI) under their control at all times. The rule makes specific references to encryption, key management, access controls, risk management and auditing.

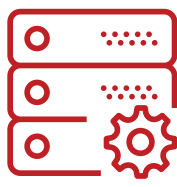


The HITECH Act, on the other hand, regulates breach notifications and requires that covered entities must inform all affected parties in case of a breach. Furthermore, under certain circumstances the act requires that media be informed if the breach involved unsecured PHI.



To further complicate matters cyber criminals are working hard to come up with new and innovative ways to breach PHI. The covered entities simply can not evolve their security strategies quickly enough to deal with these emerging threats. This is precisely why many covered entities are looking for data security services instead of a piece of software or hardware that will just encrypt their data. The Server General security service is the right solution for covered entities that want to secure their PHI quickly and comply with the HIPAA/HITECH Act. Here are some of the main techniques that are used by Server General in order to protect PHI stored within a Linux server deployed on any cloud platform.

Data Encryption



Server General uses the **Advanced Encryption Standard (AES)** algorithm to encrypt PHI. Thus we are able to meet or exceed the encryption standard requirement defined as **"AES-compatible"** by the IETF/IRTF Cipher Catalog and by the National Institute of Standards and Technology (NIST) publication FIPS 140-2.

Key Management



Key generation, storage, and distribution are always critical aspects of a key management system. Here is how our key management system works:



1 Key Generation
Our key generation procedures are designed to protect against loss, theft and compromise.



2 Key Length
We use the maximum key length possible - 256 bits.



3 Key Distribution
Our key management design forces secure distribution of the encryption keys.



4 Key Storage
We store the encryption keys in a secure key locker appliance. The appliance can be deployed on-premises or within our cloud.



5 Key Rotation
The encryption keys can be rotated without having to decrypt the encrypted data sets.



6 Key Revocation
The Server General Security Officer is able to revoke encryption keys at any time.



7 Key Custodians
Access to encryption keys is restricted to fewest number of custodians necessary.

Access Control



Today's servers are not designed with data security in mind. It is very difficult to restrict system administrator's access in a manner that does not impede their ability to do their job while disallowing them from accessing PHI stored on the server. Most network, system and cloud administrators are granted access to system resources that far exceeds any rational notion of data security. A malicious privileged insider can easily abuse their powers and gain access to PHI thereby exposing the covered entity to a HIPAA violation.

Server General protects PHI data directories by adding an additional layer of controls that prevent system administrators from gaining access to PHI in cleartext. We follow the principle of least privilege - what is not expressly permitted is denied. It should be noted that Server General is designed not to interfere with normal access control mechanisms that are provided by the application server.



1 Protection against "root"
The Server General trust model doesn't include the traditional "root" user. Thus, the "root" user is not allowed to view PHI files in cleartext.

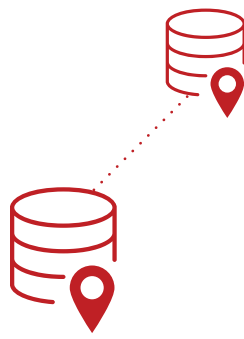


2 Separation of duties
Server General uses role-based management in order to limit access to system components and to sensitive data files to those individuals whose job requires such access.







3 Data integrity
Server General maintains integrity of PHI files through digital signatures that are computed whenever data is stored or retrieved from a protected repository.

Log Management



It is imperative for covered entities to be able to prove to their auditors that they are in full control of their PHI when it comes to access. This task is accomplished through extensive logging of all access grants and their usage. However, these log files can be easily tampered with by a malicious insider or an outsider. Server General prevents this from happening by storing each log event at two locations - a remote logging server and a local server. Since the covered entity has no control over the remote logging server, they are able to claim to their auditors that they have untainted access logs.

How do we use the above mentioned features to protect PHI?

HIPAA Requirement	Server General Feature	How Server General uses it?
45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii) "The encryption implementation specification is addressable, and must therefore be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI." ¹	 Data Encryption	Server General implements encryption at the OS layer which enables it to transparently encrypt PHI stored in a database or a file server. The algorithm used to encrypt data is AES - the same algorithm that is used by banks and the U.S. government.
164.312 (a)(2)(iv) 164.312 (e)(2)(i) "To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt." ²	 Key Management	Server General offers key management as part of its service. The encryption keys are stored in a highly secure appliances that can be deployed on-premises or within our cloud. The keys are stored away from the encrypted PHI.
"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)[Information Access Management]." ³	 Access Control	Server General uses advanced access control mechanisms that disallow unauthorized accesses to PHI using operating system exploits. System administrator (or the "root" user) is unable to view the protected PHI data sets in the cleartext format. Server General prevents malicious parties from circumnavigating the application access controls.
164.312 (b) • Audit Controls 164.308 (a)(1)(ii)(D) • Information System Activity Review	 Log Management	Server General logs every privileged operation. All log events are stored locally as well as in a remote server away from the reach of an administrator. This prevents a privileged insider from altering the log files to hide their malicious activity.

About Server General

Server General is a data security service that enables customers to protect their sensitive information stored in a Linux server and achieve regulatory compliance. The service can be used on any cloud platform - Amazon, Google or Rackspace. Customers retain full control over their own encrypted data and the associated keys.



¹ Is the use of encryption mandatory in the Security Rule?
<http://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/>
² Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
<http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>
³ 45 CFR 164.312 - Technical safeguards
<http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf>

Server General Inc. is based in New York, USA. For more information please visit www.servergeneral.com or send email to admin@servergeneral.com.