

## HIPAA Security Matrix

### Hardware Specifications:

Sections	Standards	Implementation Specifications (R)=Required, (A)=Addressable	Application Functionality
§164.308(a)(1)	Security Management Process	Risk Analysis	(R) The Covered Entity (CE) can store its Risk Analysis document encrypted and offsite using EVault® managed software solutions.
		Risk Management	(R) EVault technology provides a high degree of security by encrypting Protected Health Information (PHI) on the CE's servers. With EVault SaaS, data is transmitted over the network using additional "over-the-wire" encryption and is transferred to a secure, offsite data center thereby reducing risks and vulnerabilities for PHI. No EVault employee has access to the unencrypted PHI because the CE or business associate has the only encryption password.
		Sanction Policy	(R) EVault works with the CE to comply with sanction policies and procedures.
		Information System Activity Review	(R) Our licensed EVault Software and our EVault SaaS managed service both provide comprehensive reports for: <ul style="list-style-type: none"> <li>• Backup activity</li> <li>• Restore activity</li> <li>• Log files</li> <li>• Late backup status</li> </ul>
§164.308(a)(2)	Assigned Security Responsibility		(R) EVault Professional Services team will work with the CE's Security Officer to ensure that data protection policies adhere to the policy and procedures of the CE.

Vertical Solution  
HIPAA Security Matrix

Sections	Standards	Implementation Specifications (R)=Required, (A)=Addressable	Application Functionality
§164.308(a)(3)	Workforce Security	Authorization and/or Supervision	(A) EVault Software and EVault SaaS solutions are designed to ensure that only those personnel with appropriate application as well as encryption passwords have access to PHI.
		Workforce Clearance Procedure	(R) The CE's Security Officer determines who has access to both application and encryption passwords.
		Termination Procedures	(A) As a part of the CE's termination procedures, EVault Software and EVault SaaS solutions allow authorized CE personnel to: <ul style="list-style-type: none"> <li>• Change encryption password and</li> <li>• Change account password on the Vault</li> </ul>
§164.308(a)(4)	Information Access Management	Isolating Health Care Clearinghouse Function	(R) EVault Software and EVault SaaS solutions allow the CE to isolate data protection to authorized personnel and protect the electronic PHI (ePHI) from the larger organization.
		Access Establishment and Modification	(R) EVault Software and EVault SaaS solutions easily allow the CE to implement policies and procedures for granting access to ePHI through server as well as encryption password protection. The CE has the only password for encrypted ePHI.
		Emergency Mode Operation Plan	(R) EVault Software and EVault SaaS solutions easily allow the CE to implement policies and procedures for granting and modifying a user's access to ePHI through server as well as encryption password protection. The CE has the only password for encrypted ePHI.
§164.308(a)(5)	Security Awareness and Training	Security Reminders	(A) EVault will participate in a CE's periodic security updates on an as-needed basis.
		Protection from Malicious Software	(A) EVault Software and EVault SaaS solutions provide protection from malicious software by keeping a full copy of ePHI encrypted and offsite. A CE can easily recover uncorrupted data online, 24 hours a day.
		Log-in Monitoring	(A) EVault records log-on activity for backup and restore tasks. This activity information can be provided to the CE as needed.
		Password Management	(A) EVault backup architecture is designed specifically so that only those personnel with appropriate application as well as encryption passwords have access to PHI. CEs can encrypt and store their passwords offsite with the EVault solution.
§164.308(a)(6)	Security Incident Procedures	Response and Reporting	(R) EVault Software and EVault SaaS can mitigate harmful effects of security incidents by storing a full, encrypted copy of ePHI offsite. Through EVault's managed service, this encrypted ePHI is stored in secure data facilities.

Vertical Solution  
HIPAA Security Matrix

Sections	Standards	Implementation Specifications  (R)=Required, (A)=Addressable	Application Functionality
§164.308(a)(7)	Contingency Plan	Data Backup Plan	(R) EVault Software and EVault SaaS are specifically designed to provide CEs better operational control of their data backup and recovery process. The automated process ensures that backups have occurred and are automatically transmitted offsite. The software facilitates customized data retention schedules. The solution limits human involvement, which can lead to error in the backup process or in tape transport. The backup and recovery process can be centrally controlled (through a graphical user interface) for remote locations. Data can be instantaneously recovered 24 x 7 x 365. Data is further secured by utilizing RAID arrays and redundant components. Data is encrypted and sent to secure data centers with limited physical access.
		Disaster Recovery Plan	(R) EVault provides data protection and recovery as a part of the CE's Disaster Recovery Plan. EVault's main purpose is to protect data in the event of a full disaster or file and folder recovery. EVault will also work with the CE to test data restoration as a part of the DR Plan.
		Emergency Mode Operation Plan	(R) With EVault's managed service, data is automatically transmitted offsite and easily accessed 24 hours a day, 7 days a week. Data can be instantaneously restored while operating in an emergency mode. With EVault, data can be protected at an offsite facility of the CE's choice.
		Testing and Revision Procedure	(A) CE can contract with EVault for periodic testing of data recovery.
		Applications and Data Criticality Analysis	(A) EVault solutions easily allow the CE to identify critical data and design customized retention policies to meet the needs of other contingency plan components.
§164.308(a)(8)	Evaluation		CE can contract with EVault Professional Services for periodic evaluation of backed-up data integrity and the recovery process.
§164.308(b)(1)	Business Associate Contracts and Other Arrangement	Written Contract or Other Arrangement	(R) EVault employees do not have access to protected health information and are not considered business associates; however, EVault understands the criticality of protecting health data and will work with CEs to insure compliance with the HIPAA Act.

Vertical Solution  
HIPAA Security Matrix

Sections	Standards	Implementation Specifications (R)=Required, (A)=Addressable	Application Functionality
§164.310(a)(1)	Facility Access Controls	Contingency Operations	(A) EVault SaaS customer data is stored in vaults located in highly secure data centers that provide limited physical access but have redundant systems and power. In the event of a disaster, using EVault Software and EVault SaaS solutions, data can be recovered via the network or the public Internet to a location selected by the CE. Only authorized personnel with application and encryption passwords can recover the data.
		Facility Security Plan	(A) EVault utilizes state-of-the-art data centers with limited physical access to host vaults.
		Access Control and Validation Procedures	(A) EVault's data center partners all maintain strict procedures to limit physical access to EVault storage vaults.
		Maintenance Records	These state-of-the-art data centers feature best-in-class maintenance, security, and repair procedures.
§164.310(b)	Workstation Use		(R) n/a
§164.310(c)	Workstation Security		(R) Backed-up data is protected via application and encryption passwords that are restricted to authorized CE representatives.
§164.310(d)(1)	Device and Media Controls	Disposal	(R) Subscribers to EVault SaaS can receive a certificate that confirms that data has been deleted. Data deletion is done upon customer request only.
		Media Re-use	(R) EVault can provide a certificate to its EVault SaaS customers that confirms that data has been deleted before media is reused.
		Accountability	(A) EVault can provide to CE a record of the movements of hardware and electronic media utilized to perform backup and recovery upon request.
		Data Backup and Storage	(A) EVault Software can provide a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.
§164.312(a)(1)	Access Control	Unique User Identification	(A) EVault Software technology encrypts ePHI at the source of the information, on the CE's computer servers. Only authorized CE representatives have server and encryption passwords. The CE assigns the unique user identification.  In providing our managed data backup service, EVault SaaS, no EVault employee has access to the unencrypted PHI because the CE or business associate has the only encryption password.

Vertical Solution  
HIPAA Security Matrix

Sections	Standards	Implementation Specifications  (R)=Required, (A)=Addressable	Application Functionality
		Emergency Access Procedure	(A) EVault Software and EVault SaaS solutions are designed to provide fast, easy data recovery in case of an emergency. Access to information stored at EVault data centers can be done online at anytime. An authorized administrator at the CE can take advantage of EVault CentralControl to search through the data stored on the vault and recover the lost data online. Only the authorized system administrator can enter the vault account username and password as well as the encryption password to authenticate and get the data back.
		Automatic Logoff	(A) The EVault Software Agent scans the server on which it is installed to gather the blocks within files requiring backup. It compresses the files, encrypts them and then sends them over the network using network encryption to the storage vault. As soon as the transmission has been completed, it automatically disconnects from the customer server and logs off.
		Encryption and Decryption	(A) The Agent encrypts all data to be backed up on the server before sending it over the network. ePHI is encrypted at two levels: <ul style="list-style-type: none"> <li>• Data is encrypted on the vault to ensure that only the CE system administrator has access to the information.</li> <li>• Over-the-wire encryption ensures that the data is safe during transmission. The encryption password is entered by the system administrator while configuring the back up. If the need to recover data arises, only the system administrator can start a restore job and enter the encryption password to allow the software to bring back decrypted data to the server.</li> </ul>
§164.312(b)	Audit Control		(R) EVault records information about users who back up and restore data.
§164.312(c)(1)	Integrity	Mechanism to Authenticate Electronic Protected Health Information	(A) EVault uses two levels of authentication to protect health care information: <ul style="list-style-type: none"> <li>• Vault account authentication</li> <li>• Encryption authentication</li> </ul> <p>The CE will implement policies and procedures to ensure that ePHI has not been altered or destroyed in an unauthorized manner. If the CE finds that data has been altered on the originating server, original data can be restored online from the EVault backup. Data is destroyed only at the request of the CE. EVault will issue a certificate of data destruction if the CE requests that destruction.</p>

Vertical Solution  
HIPAA Security Matrix

Sections	Standards	Implementation Specifications  (R)=Required, (A)=Addressable	Application Functionality
§164.312(d)	Person or Entity Authentication		(R) Authentication is required to back up and recover data to and from the vault as well as to decrypt the data. <ul style="list-style-type: none"> <li>The CE's system administrator will authenticate with the vault when configuring a backup job by entering the username and password recorded on the vault.</li> <li>The user also enters an encryption password while configuring the backup job. It is impossible to decrypt the data while doing the restore without this key.</li> </ul>
§164.312(e)(1)	Transmission Security	Integrity Controls	(A) Controls can be run periodically to ensure data integrity. For example, the system administrator can run test restores to ensure that the data is intact and has not been corrupted. <p>The CE system administrator has 24x7 access to the data stored on the vault and can start restores at any time through CentralControl, an easy-to-use graphic user interface.</p>
		Encryption	(A) EVault delivers encryption in two levels at no additional cost: <ul style="list-style-type: none"> <li>Over-the-wire encryption ensures that data can't be read during transmission over a network or public Internet.</li> <li>Encryption at storage location (vault) ensures that the data can only be decrypted by the owner of the encryption key (CE entity system administrator).</li> </ul> <p>EVault utilizes the following encryption:</p> <ul style="list-style-type: none"> <li>128-bit or 256-bit AES</li> <li>56-bit or 128-bit Blowfish</li> <li>56-bit or 112-bit Triple-DES</li> </ul>

**Take the Next Step**

To learn more about EVault storage solutions, call 1.877.901.DATA (3282), email [conciierge@evault.com](mailto:conciierge@evault.com), or visit [www.evault.com](http://www.evault.com).



**Headquarters** | 3101 Jay Street, Suite 110 | Santa Clara, CA 95054 | 877.901.DATA (3282) | [www.evault.com](http://www.evault.com)  
**Netherlands (EMEA HQ)** +31 (0) 73 648 1400 | **France** +33 (0) 1 55 27 35 24 | **UK** +44 (0) 1932 445 370