



HIPAA Security Standards

choSafe data solutions – Compliance Matrix

response to the

Security Standards for the Protection of Electronic Protected Health Information
45 Code of Federal Regulations (CFR), Part 164: Security and Privacy

HIPAA Security Standards

echoSafe data solutions - Compliance Matrix

echoSafe data solutions recognize that the security and privacy of electronic health records are a primary concern of health care organizations. Using **echoSafe Backup**, our monitored backup and recovery service, the IT staff within the Covered Entity (CE) has the tools necessary to ensure the confidentiality and integrity of their Protected Health Information (PHI).

Administrative Safeguards			
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 their Risk Analysis document encrypted and off-site using echoSafe Backup.
		Risk Management (R)	echoSafe Backup provides a high degree of security by encrypting Protected Health Information (PHI) on the CE's servers prior to transmitting the data over the network to echoSafe's secure, offsite data center. This reduces the risks and vulnerabilities for PHI. No echoSafe employee has access to the unencrypted PHI because the covered entity or business associate has the only encryption password.
		Sanction Policy (R)	echoSafe works with the CE to comply with their sanction policies and procedures.
		Information System Activity Review (R)	Our licensed software, echoSafe Backup provide comprehensive reports for: <ul style="list-style-type: none"> • Backup activity • Restore activity • Log files • Late backup status
§164.308(a)(2)	Assigned Security Responsibility	(R)	echoSafe data solutions will work with the CE's Security Officer to ensure that data protection policies adhere to the policy and procedures of the CE.
§164.308(a)(3)	Workforce Security	Authorization and/or Supervision (A)	echoSafe's software and service solutions are designed to ensure that only those personnel with account names, login passwords, and encryption passwords have access to PHI.
		Workforce Clearance Procedure (A)	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, echoSafe Backup allows authorized CE personnel to change encryption passwords.

HIPAA Security Standards

echoSafe data solutions - Compliance Matrix

Administrative Safeguards			
Sections	Standards	Implementation Specifications (R)=Required, (A)=Addressable	Application Functionality
§164.308(a)(4)	Information Access Management	Isolating Health Care Clearinghouse Functions (R)	echoSafe Backup allows the CE to isolate data protection to authorized personnel and protect the electronic PHI (ePHI) from the larger organization.
		Access Authorization (A)	echoSafe Backup will 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.
		Access Establishment and Modification (A)	echoSafe Backup will 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.
§164.308(a)(5)	Security Awareness and Training	Security Reminders (A)	echoSafe data solutions will participate in a CE's periodic security updates on an as needed basis.
		Protection from Malicious Software (A)	echoSafe Backup provides protection from malicious software by keeping a full copy of ePHI encrypted and off-site. A CE can easily recover their uncorrupted data online, 24 hours a day.
		Log-in Monitoring (A)	echoSafe Backup records all transaction activity for backup and restore tasks. This activity information can be provided to the CE as needed.
		Password Management (A)	echoSafe Backup is designed specifically so that only those personnel with the backup software, as well as encryption passwords have access to PHI.
§164.308(a)(6)	Security Incident Procedures	Response and Reporting (R)	echoSafe Backup can mitigate harmful effects of security incidents by storing a full, encrypted copy of ePHI off-site in a secure data center.

HIPAA Security Standards

echoSafe data solutions - Compliance Matrix

Administrative Safeguards			
Sections	Standards	Implementation Specifications (R)=Required, (A)=Addressable	Application Functionality
§164.308(a)(7)	Contingency Plan	Data Backup Plan (R)	echoSafe Backup is designed to give CE's complete control of the EPHI backup and recovery process. The software automatically moves backup data to a secure off-site location, and eliminates potential data loss from human error. The software also allows for customizable data retention plans. All data can be recovered 24/7/365 through a broadband internet connection. echoSafe data solutions can also bring a full copy of the data to the CE's site for fast retrieval of all data. Data is protected at echoSafe's data center with mirrored RAID arrays, as well as automated tape backup. The echoSafe data center has limited physical access and is monitored 24 hours a day by CCTV.
		Disaster Recovery Plan (R)	echoSafe Backup provides data backup and recovery as a part of the CE's Disaster Recovery Plan. echoSafe data solutions will also work with the CE to test data restoration as a part of the DR Plan.
		Emergency Mode Operation Plan (R)	echoSafe Backup stores EPHI securely off-site. The EPHI can be accessed 24/7/365 by the CE from any location, including an emergency mode operating location.
		Testing and Revision Procedures (A)	echoSafe Backup is designed to allow the CE to periodically test the EPHI data recovery process without disturbing the existing on-line data. echoSafe data solutions can also be contracted to perform this task.
		Applications and Data Criticality Analysis (A)	echoSafe Backup will allow the CE to easily identify critical data, and design customized retention policies to meet the needs of other contingency plan components.
§164.308(a)(8)	Evaluation	(R)	CE can contract with echoSafe data solutions for periodic evaluation of backed up data integrity and the recovery process.
§164.308(b)(1)	Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement (R)	echoSafe data solution employees do not have access to protected health information and is not considered a business associate; however, echoSafe data solutions understands the criticality of protecting health data and will work with Covered Entities to insure their compliance with the HIPAA Act.

HIPAA Security Standards

echoSafe data solutions - Compliance Matrix

Physical Safeguards			
Sections	Standards	Implementation Specifications (R)=Required, (A)=Addressable	Application Functionality
§164.310(a)(1)	Facility Access Controls	Contingency Operations (A)	echoSafe Backup customer data is stored in a secure data center with redundant power, cooling, and internet access. In the event of a disaster, only authorized personnel with application and encryption passwords can recover the data.
		Facility Security Plan (A)	echoSafe utilizes a secure data center for all its equipment
		Access Control and Validation Procedures (A)	echoSafe's data center partner maintains strict procedures to limit physical access to the data center and to validate a person's access.
		Maintenance Records (A)	These state-of-the-art data centers have best in class maintenance, security, and repair procedures.
§164.310(b)	Workstation Use		n/a
§164.310(c)	Workstation Security		Data that is backed up 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 echoSafe Backup can receive a certificate that confirms that data has been deleted. Data deletion is done upon customer request only.
		Media Re-use (R)	echoSafe data solutions can provide a certificate to its echoSafe Backup customers that confirms that data has been deleted before media is reused.
		Accountability (A)	echoSafe data solutions 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)	echoSafe Backup can provide a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.

HIPAA Security Standards

echoSafe data solutions - Compliance Matrix

Technical Safeguards			
Sections	Standards	Implementation Specifications (R)=Required, (A)=Addressable	Application Functionality
§164.312(a)(1)	Access Control	Unique User Identification (R)	<p>echoSafe Backup 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.</p> <p>No echoSafe data solutions employee has access to the unencrypted PHI because the CE or business associate has the only encryption password.</p>
		Emergency Access Procedure (R)	<p>echoSafe Backup is designed to provide fast, easy data recovery in case of an emergency. Access to information stored at the echoSafe data center can be done online at anytime. An authorized administrator at the CE can take advantage of echoSafe Backup to search through the data stored on the backup servers and recover the lost data online. Only the authorized system administrator can enter the account username and password as well as the encryption password to authenticate and get the data back.</p>
		Automatic Logoff (A)	<p>The echoSafe Backup software scans the server on which it is installed to gather the data requiring backup. This data is compressed and encrypted before is sent over the network to the backup server. As soon as the transmission has been completed, it automatically disconnects from the customer server and logs off.</p>
		Encryption and Decryption (A)	<p>echoSafe Backup encrypts all data to be backed up on the server before sending them over the network. The data is encrypted on the customer server to ensure that only the covered entity system administrator has access to the information as he is the only owner of the encryption password. The encryption password is entered by the system administrator while configuring the backup. 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.</p>

HIPAA Security Standards

echoSafe data solutions - Compliance Matrix

Technical Safeguards			
Sections	Standards	Implementation Specifications (R)=Required, (A)=Addressable	Application Functionality
§164.312(b)	Audit Controls		echoSafe data solutions records information about users who backup and restore data.
§164.312(c)(1)	Integrity	Mechanism to Authenticate Electronic Protected Health Information (A)	<p>echoSafe Backup software uses 2 levels of authentication to protect Health Care Information:</p> <ul style="list-style-type: none"> • echoSafe Backup account authentication • Encryption authentication <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 on line from echoSafe Backup. Data is destroyed only at the request of the CE. echoSafe data solutions will issue a certificate of data destruction if the CE requests that destruction.</p>
§164.312(d)	Person or Entity Authentication		<p>Authentication is required to backup and recover data to and from the backup server as well as to decrypt the data.</p> <ul style="list-style-type: none"> • The CE's system administrator will authenticate with the backup server when configuring a backup job by entering the username and password recorded on the backup server. • The user also enters an encryption password while configuring the backup job. He is the only one that knows this key and it will be impossible to decrypt the data while doing the restore without it.
§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. The CE system administrator has 24/7 access to the data stored on the backup server and can start restores at any time through echoSafe Backup's easy-to-use graphic user interface.
		Encryption (A)	All data backed up through echoSafe Backup is encrypted using the US Government backed Advanced Encryption Standard (128bit AES)