Axcient

White Paper: HIPAA Compliance

A Guide for Companies Using Axcient Services to Facilitate HIPAA and Hitech Compliance.

HIPAA & HITECH Overview

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in 1996 to improve insurance portability (Title I), as well as to reduce fraud and simplify administration (Title II). Title II establishes data security and privacy standards for the transmission, storage, and disclosure of individually identifiable health information, termed protected health information (PHI) and electronic PHI (ePHI). HIPAA regulations apply to any "covered entity," which includes health plans, health care clearinghouses, and any health care provider who uses or transmits electronic personally identifiable health information (Covered Entities). HIPAA was expanded in 2009 through the Health Information Technology for Economic and Clinical Health Act (HITECH). In 2013, the final HIPAA Omnibus rule further expanded HIPAA so that all custodians of PHI (not just Covered Entities), including HIPAA Business Associates (BA), are subject to the same security and data privacy rules of Covered Entities under HIPAA and HITECH. Axcient is considered a Business Associate under the law, and will sign BA agreements.

HIPAA Privacy Rule

The Privacy Rule establishes requirements and procedures that covered entities and their business associates must meet when storing or transmitting any protected health information (PHI). The rule restricts when and how an individual's protected health information may be used or disclosed. An individual's PHI may only be disclosed (a) to the individual whom is the subject of the PHI (or their authorized agent), (b) to the U.S. Department of Health and Human Services (HHS) as part of an audit or review, (c) as has been otherwise authorized in writing by the individual whom is the subject of the PHI, (d) as part of a covered entity's treatment, payment, and health care operations activities, or (e) other specific circumstances as detailed in the Privacy Rule. Non-compliance with the privacy rule carries civil and criminal penalties. The deadline for compliance with the Privacy Rule was April 14th, 2003.

HIPAA Security Rule

The Security Rule defines standards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). Specifically, HIPAA § 164.306 requires that organizations:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
4. Ensure compliance by its workforce.

More specific requirements are defined to meet the above objectives, including Administrative Safeguards, Physical Safeguards, Technical Safeguards, Organizational Requirements, and Documentation Requirements. Covered entities are given the flexibility to implement the requirements in reasonable and appropriate ways that best fit within that organization that also mitigate the potential risks to ePHI. Organizations are required to perform risk analysis, maintain documentation of its implementation of the Security Rule, and monitor and audit the effectiveness of its controls.

A key part of the administrative safeguards (HIPAA § 164.308) is the written contingency plan, which requires that organizations have a reasonable plan for ensuring the integrity and availability of ePHI in the event of an emergency or disaster. This plan must provide details on the mechanisms used for data backup and disaster recovery and how these mechanisms comply with the Security Rule.

How Axcient Helps Organizations Comply with HIPAA & HITECH

Axcient's cloud, and certain Axcient services that run on Axcient's cloud, meet the obligations required by HIPAA and HITECH to pr otect the privacy and security of ePHI, guarding ag ainst those risks that are within our scope of responsibility to control. Axcient has extensive security controls and systems as required by HIPAA to safeguard your data, including physical, network, operational, and administrative controls.

Axcient will sign business associate agreements (BAA) with any organization for Axcient services that are documented to be eligible for HIPAA compliance. Partners and their end-user customers are responsible for configuring Axcient services to meet requirements of HIPAA within their specific environment (as determined by their own internal or external compliance audits), and for forming and enforcing policies in their organizations to be HIPAA compliant. Axcient provides guidance to assist in, but not guarantee, configuring compliant configurations.

Additionally, Axcient's secure data protection services help partners and their customers meet HIPAA regulations. HIPAA's contingency plan requirement specifies that organizations must implement a data backup and disaster recovery plan that protects electronic protected health information (ePHI) while mitigating risks to the disclosure of ePHI. Certain Axcient services can be used as a central part of this plan to automatically and cost-effectively protect ePHI data and provide fast data recovery, while also meeting HIPAA's data privacy, confidentiality, integrity, and availability requirements.

Which Axcient services are HIPAA & HITECH compliant?

Axcient has a broad portfolio of data protection and cloud storage services. While Axcient maintains the highest standard of data security, availability, and integrity for all of our services, not all of our services have been included within the scope of our HIPAA audits.

HIPAA & HITECH Compliance of Axcient Products

SERVICES	STATUS	STATUS
x360Sync	Compliant	See minimum security baseline guidelines
Backup for Files	Compliant	See minimum security baseline guidelines
BRC	Compliant for NEW installations of Version 7.0 or newer	See minimum security baseline guidelines
x360Recover	Compliant	See minimum security baseline guidelines
x360Cloud	Compliant	See minimum security baseline guidelines

Minimum Security Baselines

It is the responsibility of any organization that uses Axcient's services to ensure that they are doing so in such a way that is HIPAA compliant within their specific environment. To help organizations understand how to leverage certain Axcient services facilitate or maintain HIPAA compliance, we have made available guidance on how such services must be configured at a minimum in order to operate in a HIPAA compliant fashion.

A configuration that does not match the minimum security baseline is not compliant, and thus it is critical that organizations configure Axcient services to at least match the minimum security baseline. Note that configuring Axcient services to match the minimum security baseline does not guarantee compliance, and organizations should work with their auditors to ensure that Axcient services are compliant within the context of their specific IT environment. Axcient is ready to speak with you and your auditors to discuss compliance, and our rigorous systems & controls that facilitate compliance.

The recommended minimum security baseline for each Axcient service that is eligible for HIPAA compliance will be documented in a separate section. Any configuration-related requirement will be labeled with (CFG). Any organizational environmental requirement will be labeled with (ENV).

x360Sync: Minimum Security Baseline Guidelines

Axcient x360Sync provides file synchronization and secure anytime, anywhere access to your file-level data. Data is synchronized from server, desktop, laptop, and mobile endpoints to the cloud, where it can be securely accessed and further shared according to configured policy. Data is encrypted in-transit and at-rest, using encryption keys that are managed by Axcient. Enforced two-factor authentication provides strong authentication, and configurable access control features can prevent unauthorized access to ePHI.

Server, Desktop, & Laptop Endpoints (ENV):

- The file system that you connect to the x360Sync sync agent to store synchronized file data must utilize at-rest encryption that is HIPAA compliant.
- You must have controls in place that ensure that any local access to ePHI stored on these endpoints is properly protected and audited as required by HIPAA, including ePHI data that may exist on the endpoint through the use of the x360Sync agent.

Mobile Endpoints (ENV):

- All mobile endpoints must use Device encryption such that all data on the mobile endpoint (phone, tablet, etc.) is encrypted using an algorithm that is HIPAA compliant. Such encryption must be strong enough and configured in such a way that the loss or theft of the mobile endpoint would not be considered a breach of ePHI under HIPAA.
- You must use a mobile-device-management (MDM) solution that preserves access records to any ePHI data that is stored on the device, including ePHI that could be downloaded through the use of the x360Sync application.

Data Encryption at Rest:

In the cloud: Data is encrypted, using 256-bit AES Encryption on data at-rest within the Axcient cloud. Encryption keys are managed by Axcient. Use and access to such encryption keys are tightly controlled, and such encryption keys are furthermore themselves stored encrypted.

On the endpoint (ENV): Refer to the endpoint requirements above for details.

Data Encryption in Transit:

All communications are automatically encrypted when in transit over the network using the TLS protocol using encryption ciphers that comply with HIPAA requirements.

Authentication:

Overview: Users authenticate with the x360Sync system using a username and password, and optionally two-factor authentication as well. Sync agents on endpoints authenticate registration of the device through user-level authentication, after which they authenticate through certificate a based authentication token unique to the endpoint.

- **(CFG):** Configure a password that is strong & unique.
- **(CFG):** Enable the two-factor authentication feature, and configure your organizational settings to require all users to setup two-factor authentication.
- **(ENV+CFG):** Your mobile endpoint's own authentication and lock screen features must be configured according to your organization's policy to protect ePHI, these can be enforced in your MDM. The x360Sync application on mobile endpoints can be configured to provide further protection by requiring a pass code either immediately on accessing the application or after a reasonable idle timeout. The setting to erase data after 10 failed pass code attempts must be enabled. Both of these settings can be managed at the admin level by enabling Two-Step authentication.

Access Control:

- **Overview:** x360Sync allows access to data only according to policies configured by users.
- **(CFG):** "Privacy mode" must be configured within x360Sync to ensure administrators cannot view user files within synced tool.
- **(CFG)**: Anonymous share links must never be configured for files that contain ePHI. Instead, always use the Team Share or Secure Share feature to share data, and only with those parties that are authorized to access the ePHI that is being shared with them.

Audit Logging:

- Axcient preserves an audit log of changes to configuration or data, and is viewable from within x360Sync. Access logs are kept for any anonymous or authenticated user that downloads data from the x360Sync web portal or a mobile endpoint.
- **(ENV):** Your environment must keep an appropriate audit log of all access to ePHI data on the endpoints themselves, including server, desktop, laptop, and mobile.

Backup for Files: Minimum Security Baseline Guidelines

Axcient Backup for Files provides cloud, disk-to-disk, and cross-network backup of file-level data. Data is encrypted in-transit and at-rest, using an encryption key not known to Axcient. All data access is authenticated, and then is further protected by knowledge of the encryption key.

Source Data (ENV):

The data being backed up by Backup for Files must be protected and safeguarded to meet HIPAA compliance if it contains ePHI. The Backup for Files service does not affect compliance of the source data itself (or restored data), as it is only making a copy of your data. Make sure that you are compliant with HIPAA requirements to protect your data prior to deploying this service.

Data Encryption at Rest:

- **Overview:** Data is encrypted at the client prior to transmission to the cloud or other backup destination, using a private encryption key chosen by your organization. Data is only decrypted during a restore after it has been received from the network.

- **Encryption Key (CFG):** You must configure the backup manager with an encryption key that is known only to the organization that is authorized to access the ePHI. You must choose an encryption pass-phrase that will generate a sufficiently strong encryption key. You must protect this encryption key to prevent unauthorized disclosure.
- **Cloud Backups:** All cloud backups must always have at-rest encryption enabled.
- **Cross-Network or Local D2D Backups (CFG):** You must ensure that the data encryption option is enabled on the My Account page i**n the backup manager for local backups.**

Data Encryption in Transit:

- All communications are automatically encrypted when in transit over the network using the TLS protocol. Furthermore, all backed up data will further be encrypted with another layer of encryption when in transit, providing two layers of encryption for customer data over the wire.

Authentication (CFG):

- Data backed up to the cloud is associated with an account that is authenticated via a username and password. Configure a password that is strong & unique.

Access Control:

All backed up data can only be accessed by the authenticated user associated with the data, and is further controlled by knowledge of the encryption pass-phrase.

- **(ENV):** Do not disclose the credentials or encryption pass-phrase to unauthorized parties.

Audit Logging:

- Axcient preserves an audit log of all backed up data, data restores, and configuration changes, and can be provided on demand as necessary.
- **(ENV):** You must keep an audit trail anytime account credentials or the encryption key are disclosed.
- **(ENV):** Your environment must keep an appropriate audit log of all access to ePHI data that is either in the original source data being backed up, or is in data that you restore.

Data Restores (ENV):

You must only restore ePHI data to systems that have the proper data privacy, authentication, access control, and audit logging controls in place to safeguard the restored ePHI.

Seeding Service (ENV):

The Backup for Files agent always encrypts, at-rest, any data stored to a “seed device” that you may then ship to Axcient. Make sure that you do not store your encryption pass-phrase on the physical media, or otherwise include it within the package that is shipped to Axcient. Follow all current seeding procedures described in the Axcient support knowledge base. This is critical to ensuring HIPAA compliance of seed drives.

x360Recover: Minimum Security Baseline Guidelines

Axcient x360Recover provides local and cloud backup of volume-level data (entire servers and desktops). Data is encrypted in-transit and at-rest, using an encryption key not known to Axcient. All data access is authenticated, and then further protected by knowledge of the encryption key. Components to the x360Recover infrastructure include the Local Agent, Appliance, Vault, License Portal and Global Management Portal.

Source Data (ENV):

The data being backed up must be protected and safeguarded to meet HIPAA compliance if it contains ePHI. This Axcient service does not affect compliance of the source data itself (or restored data), as it is only making a copy of your data. Make sure that you are compliant with HIPAA requirements to protect your data prior to deploying this service.

Data Encryption at Rest

- **Overview:** Data is encrypted client-side prior to transmission to the cloud or other backup destination. Data is only decrypted during a restore after it has been received from the network. **NOTE: Only x360Recover installations that utilize the Axcient Cloud Key Management (CKMS) are approved for use in a HIPAA regulated environment. Please check with your account manager to ensure this is properly configured on your local and cloud x360Recover solutions.
- **Cloud Backups:** By configuring encryption on your backups you are ensuring that cloud backups have at-rest encryption enabled as well.

Data Encryption in Transit (CFG):

All communications are automatically encrypted when in transit over the network using the TLS protocol. Furthermore, all backed up data will further be encrypted with another layer of encryption when in transit, providing two layers of encryption for customer data over the wire.

- **Email Notices:** If notifications are desired from the x360Recover Appliance, Vault or GMP, rest assured no backup data will be contained within that notice. However, since the notice will detail potentially sensitive information about devices containing HIPAA related data it is imperative that emails are sent using encryption. Both the “StartTLS” and the “SSL/TLS” enforce opportunistic encryption from the devices. This setting can be found under the email settings in the Connection Security drop down menu. NOTE: your email server or relay will have to be configured to relay these email messages and force encryption.

Authentication (CFG):

Data backed up to the cloud is associated with an account that is authenticated via the username and password assigned to the customer. When creating your customer accounts within the x360Recover License Portal, ensure that each password is strong & unique and meets or exceeds HIPAA requirements.

Access Control:

All backed up data can only be accessed by the authenticated user associated with the data, and is further controlled by knowledge of the encryption pass-phrase.

- **(ENV):** Do not disclose the credentials or encryption pass-phrase to unauthorized parties.
- **(CFG):** Enable the x360Recover host firewall by navigating to Settings>Network Settings> then check "Enable Firewall"
- **(CFG):** Enable x360Recover Auto Updates by navigating to Settings>Update Manager> the check "Enable Auto Update"

Audit Logging:

Axcient preserves an audit log of all backed up cloud data, cloud data restores, and cloudconfiguration changes, and can be provided on demand as necessary.

- **(ENV):** You must keep an audit trail anytime account credentials or the encryption key are disclosed.
- **(ENV):** Your environment must keep an appropriate audit log of all access to ePHI data that is either in the original source data being backed up, or is in data that you restore.
- **Data Restores (ENV):** You must only restore ePHI data to systems that have the proper data privacy, authentication, access control, and audit logging controls in place to safeguard the restored ePHI.

Seeding Service (ENV):

Backup data must always be encrypted both at rest and in transit. x360Recover automatically encrypts all data transferred over the wire as well as at rest. When using a USB "seed device" to transfer bulk data to the Axcient cloud the data will be encrypted automatically using the customer account password that was created within the x360Recover License Portal. It is essential to make sure that each customer account password is both strong and unique. Follow all current seeding procedures described in the Axcient support knowledge base. This is critical to ensuring HIPAA compliance and the security of your seed drives and sensitive data.

x360Cloud: Minimum Security Baseline Guidelines

Axcient x360Cloud provides cloud backup, search, restore, and reporting functionality for file-level data. Data is encrypted in-transit and at-rest, using encryption keys managed by Axcient. All data access is authenticated, and configurable access control features can prevent unauthorized access to ePHI.

Source Data (ENV):

The data being backed up must be protected and safeguarded to meet HIPAA compliance if it contains ePHI. This Axcient service does not affect compliance of the source data itself (or restored data), as it is only making a copy of your data. Make sure that you are compliant with HIPAA requirements to protect your data prior to deploying this service.

Data Encryption at Rest:

- **Overview:** Proper configurations should ensure that data is encrypted client-side prior to transmission to the cloud or other backup destination, using a private encryption key chosen by your organization. Data is only decrypted during a restore after it has been received from the network.

Data Encryption in Transit:

All communications are automatically encrypted when in transit over the network using the TLS protocol.

Authentication (CFG):

Data backed up to the cloud is associated with an account that is authenticated via a username and password. Configure a password that is strong and unique. Access Control: x360Cloud allows access to data only according to policies configured by users.

- **(ENV):** Do not disclose credentials to unauthorized parties.

Audit Logging:

x360Cloud preserves an audit log of all backed up data and data restores, which can be provided on-demand as necessary.

- **(ENV):** You must keep an audit trail anytime account credentials or the encryption key are disclosed.
- **(ENV):** Your environment must keep an appropriate audit log of all access to ePHI data that is either in the original source data being backed up or is in data that you restore.

Data Restores (ENV):

You must only restore ePHI data to systems that have the proper data privacy, authentication, access control, and audit logging controls in place to safeguard the restored ePHI.

BRC: Minimum Security Baseline Guidelines

Axcient BRC provides cloud backup, search, and restore functionality for file-level data. Data is encrypted in-transit and at-rest, using an encryption key not known to Axcient. All data access is authenticated and then is further protected by knowledge of the encryption key.

Source Data (ENV):

The data being backed up must be protected and safeguarded to meet HIPAA compliance if it contains ePHI. This Axcient service does not affect compliance of the source data itself (or restored data), as it is only making a copy of your data. Make sure that you are compliant with HIPAA requirements to protect your data prior to deploying this service.

Data Encryption at Rest:

- **Overview:** Proper configurations should ensure that data is encrypted client-side prior to transmission to the cloud or other backup destination, using a private encryption key chosen by your organization. Data is only decrypted during a restore after it has been received from the network. Data Encryption in Transit: All communications are automatically encrypted when in transit over the network using the TLS protocol. Furthermore, all backed up data will be encrypted with another layer of encryption when in transit, providing two layers of encryption for customer data over the wire.

Authentication (CFG):

Data backed up to the cloud is associated with an account that is authenticated via a username and password. Configure a password that is strong and unique.

Access Control:

All backed up data can only be accessed by the authenticated user associated with the data and is further controlled by knowledge of the encryption pass-phrase.

- **(ENV):** Do not disclose the credentials or encryption pass-phrase to unauthorized parties.

Audit Logging:

All BRC appliance activity is logged by the Remote Web Console (RMC). Customers can generate their own audit reports via the RMC for logs within the last year, or support can generate reports for logs older than one year.

- **(ENV):** You must keep an audit trail anytime account credentials or the encryption key are disclosed.
- **(ENV):** Your environment must keep an appropriate audit log of all access to ePHI data that is either in the original source data being backed up or is in data that you restore.

Data Restores (ENV):

You must only restore ePHI data to systems that have the proper data privacy, authentication, access control, and audit logging controls in place to safeguard the restored ePHI.

Seeding Service (ENV):

The BRC agent always encrypts, at-rest, any data stored to a “seed device” that you may then ship to Axcient. Make sure that you do not store your encryption pass-phrase on the physical media, or otherwise include it within the package that is shipped to Axcient. Follow all current seeding procedures describe.

Conclusion

Axcient is committed to providing cloud services that are secure and reliable, and that will facilitate your organization’s compliance with HIPAA and HITECH. Please reach out to us to discuss further details or concerns. To sign a HIPAA business associate agreement with Axcient, please contact your account manager.

Disclaimer

This white paper is not intended as legal advice. You are advised to seek legal counsel to ensure compliance with laws that may affect your business, including HIPAA and HITECH. Axcient Inc and its affiliated entities make no warranties, representations, nor guarantees that your use of our services will assure compliance with any applicable laws, including but not limited to HIPAA and HITECH.

Axcient

ABOUT AXCIENT:

Axcient is an award-winning leader in business continuity and disaster recovery for Managed Service Providers (MSPs). Axcient x360 provides one platform for MSPs to Protect Everything™, and includes BCDR, Microsoft 365 and Google Workspace backup, and secure sync and share. Trusted by more than 3,000 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

CONTACT:

Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202 | Phone: 720-204-4500

FOLLOW US:

axcient.com