# eFolder White Paper: HIPAA Compliance

November 2015

## Abstract

This paper outlines how companies can use certain eFolder services to facilitate HIPAA and HITECH compliance within their organizations. Certain eFolder services can be used to help fulfill certain requirements of HIPAA, such as requirements for backup of data or disaster recovery preparedness. Furthermore, this paper overviews eFolder's own internal controls for data security and privacy, and provides recommendations on how companies can leverage certain eFolder services to fulfill their own data security and privacy obligations under HIPAA and HITECH.

## 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. eFolder 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. The deadline for compliance with the Security Rule was April 21st, 2005.

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 eFolder Helps Organizations Comply with HIPAA & HITECH

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

eFolder will sign business associate agreements (BAA) with any organization for eFolder services that are documented to be eligible for HIPAA compliance. Partners and their end-user customers are responsible for configuring eFolder 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. eFolder provides guidance to assist in, but not guarantee, configuring compliant configurations.

Additionally, eFolder'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 eFolder 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 eFolder services are HIPAA & HITECH compliant?

eFolder has a broad portfolio of data protection and cloud storage services. While eFolder 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.

| Service | Status | Further Comments |
|---|---|---|
| Anchor | Compliant | See minimum security baseline guidelines |
| Backup for Files | Compliant | See minimum security baseline guidelines |
| BDR for Acronis | Compliant | See minimum security baseline guidelines |
| BDR for AppAssure (V5) | Compliant | See minimum security baseline guidelines |
| BDR for ShadowProtect | Compliant | See minimum security baseline guidelines |
| BDR for Veeam | Compliant | See minimum security baseline guidelines |
| Continuity Cloud | Compliant | See minimum security baseline guidelines |
| Cloudfinder | Under Review | Service is expected to be compliant; an audit is underway |
| DoubleCheck | Not Applicable | Email should never contain ePHI; HIPAA is not applicable |

## Minimum Security Baselines

It is the responsibility of any organization that uses eFolder'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 eFolder 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 eFolder services to at least match the minimum security baseline. Note that configuring eFolder services to match the minimum security baseline does not guarantee compliance, and organizations should work with their auditors to ensure that eFolder services are compliant within the context of their specific IT environment. eFolder 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 eFolder 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)**.

## Anchor: Minimum Security Baseline Guidelines

eFolder Anchor 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 eFolder. Enforced two-factor authentication provides strong authentication, and configurable access control features can prevent unauthorized access to ePHI.

- **Server, Desktop, & Laptop Endpoints (ENV):**
  - The filesystem that you connect to the Anchor 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 Anchor 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 Anchor app.
- **Data Encryption at Rest:**
  - **In the cloud:** Data is encrypted, using 256-bit AES Encryption on data at-rest within the eFolder cloud. Encryption keys are managed by eFolder. 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 Anchor 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 lockscreen features must be configured according to your organization's policy to protect ePHI. The Anchor app on mobile endpoints can be configured to provide further protection by requiring a passcode either immediately on accessing the app or after a reasonable idle timeout. The setting to erase data after 10 failed passcode attempts must be enabled.

- **Access Control:**
  - **Overview:** Anchor allows access to data only according to policies configured by users.

  - **(CFG):** "Privacy mode" must be configured 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:**
  - eFolder preserves an audit log of changes to configuration or data, and is viewable from within Anchor. Access logs are kept for any anonymous or authenticated user that downloads data from the Anchor 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

eFolder 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 eFolder. 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 passphrase that will generate a sufficiently strong encryption key. You must protect this encryption key to prevent unauthorized disclosure.

  - **Cloud Backups:** All cloud backups 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 in 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 passphrase.

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

- **Audit Logging:**
  - eFolder 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 then shipped to eFolder in order. Make sure that you do not store your encryption pass phrase on the physical media, or is otherwise contained within the package that is shipped to eFolder. Follow all current seeding procedures described in the eFolder support knowledgebase. This is critical to ensuring HIPAA compliance of seed drives.

# BDR for Acronis: Minimum Security Baseline Guidelines

eFolder BDR for Acronis 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 eFolder. All data access is authenticated, and then 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 eFolder 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, using a private encryption key chosen by your organization. Data is only decrypted during a restore after it has been received from the network.

  - **Enable Acronis Encryption (CFG):** Enable encryption by clicking the blue "Encryption" link in the main window. The vault encryption dialog box will appear. In the "Select the encryption algorithm" dropdown list, select AES 256. You will need to enter a strong encryption word or phrase that complies with HIPAA requirements.

  - **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:** 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 passphrase.
  - **(ENV):** Do not disclose the credentials or encryption passphrase to unauthorized parties.
- **Audit Logging:** eFolder 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 then shipped to eFolder in order. Make sure that you do not store your encryption pass phrase on the physical media, or is otherwise contained within the package that is shipped to eFolder. Follow all current seeding procedures described in the eFolder support knowledgebase. This is critical to ensuring HIPAA compliance of seed drives.

# BDR for AppAssure: Minimum Security Baseline Guidelines

eFolder BDR for AppAssure provides local, cross-site, 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 eFolder. All data access is authenticated, and then 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 eFolder 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:** When properly configured, 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.

  - **Enable AppAssure Encryption (CFG):** You must choose to enable encrypted backups within the AppAssure V5 CORE, and use encryption for all backups.

  - **Encryption Key (CFG):** You must configure the AppAssure with an encryption key that is known only to the organization that is authorized to access the ePHI. You must choose an encryption passphrase that will generate a sufficiently strong encryption key. You must protect this encryption key to prevent unauthorized disclosure.

  - **Preventing Access to the Encryption Key (CFG):** The AppAssure CORE has a feature that allows you to "unlock" the encryption key and keep it in RAM for a period of time (or even unlocked permanently and stored on-disk). For the AppAssure CORE that is running within the eFolder cloud, you must not permanently unlock your encryption key. You must only unlock the encryption key during the short period of time when you are doing a restore operation.

- **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 & 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 passphrase.

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

- **Audit Logging:**
  - eFolder preserves an audit log of all backed up data and data restores, 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+CFG):** You must ensure that AppAssure is configured to encrypt all backups. Make sure that you do not store your encryption pass phrase on the physical media, or is otherwise contained within the package that is shipped to eFolder. Follow all current seeding procedures described in the eFolder support knowledgebase. This is critical to ensuring HIPAA compliance of seed drives.

# BDR for ShadowProtect: Minimum Security Baseline Guidelines

eFolder BDR for ShadowProtect 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 eFolder. All data access is authenticated, and then 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 eFolder 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, using a private encryption key chosen by your organization. Data is only decrypted during a restore after it has been received from the network.

  - **Enable ShadowProtect Encryption (CFG):** Configure ShadowProtect to encrypt your local ShadowProtect backups with a strong encryption pass phrase known only to those authorized to access the ePHI.

  - **Backup for Files Encryption Key (CFG):** You must configure the eFolder Backup for Files agent that sends the ShadowProtect data to the eFolder cloud with an encryption key that is known only to the organization that is authorized to access the ePHI. You must choose an encryption passphrase that will generate a sufficiently strong encryption key. You must protect this encryption key to prevent unauthorized disclosure.

  - **Cloud Backups:** All cloud backups 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 in the Backup for Files 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 passphrase.

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

- **Audit Logging:**
  - eFolder preserves an audit log of all data backed up to the cloud, data restores from the cloud, and configuration changes of the Backup for Files agent, 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 that is responsible for sending ShadowProtect data to the eFolder cloud always encrypts at-rest any data stored to a "seed device" that you then shipped to eFolder in order. Make sure that you do not store your encryption pass phrase on the physical media, or is otherwise contained within the package that is shipped to eFolder. Follow all current seeding procedures described in the eFolder support knowledgebase. This is critical to ensuring HIPAA compliance of seed drives.

# Continuity Cloud: Minimum Security Baseline Guidelines

The eFolder Continuity Cloud is a general purpose IAAS service that makes it possible for partners to provide HIPAA compliance disaster recovery services to their clients. The Continuity Cloud provides virtual router/firewall, compute, and storage resources to enable organizations to run their backed up servers or other virtual machine workloads as necessary during a disaster recovery or DR-test scenario.

- **Network Security (CFG):** The virtual router/firewall must be configured to meet the security requirements of HIPAA & HITECH for any OS or other service you have configured to run in the Continuity Cloud.

- **Data Encryption at Rest:**
  - **Overview:** The same data encryption mechanisms used in a traditional computing environment, such as OS-level or filesystem-level encryption, can also be used within the Continuity Cloud to encrypt data at rest. The Continuity Cloud provides organizations full administrative access over their computing environments, allowing you to configure these at-rest encryption mechanisms as you normally would to protect your ePHI data.

  - **Use at-rest encryption (ENV+CFG):** You must ensure that for any VM you run in the Continuity Cloud that contains ePHI, that VM must use some form of at-rest encryption of data. This could be full-disk encryption software running within the VM itself, or it can be accomplished by deploying at-rest encryption onto the Continuity Cloud itself where the VM's virtual hard disk is stored. For example, BitLocker or another full-disk-encryption software package could be used to fully encrypt the entire X: data volume on your Continuity Cloud node. No matter which full-disk encryption solution is used, it must be configured so that every time the Continuity Cloud node reboots, the data volume will not be accessible until a user manually enters an encryption key to unlock the encrypted volume.

- **Data Encryption in Transit (ENV+CFG):** The Continuity Cloud is providing the raw networking infrastructure resources that your VMs and applications can use to connect back to the Internet. You must ensure that for any VMs/applications you run within the Continuity Cloud that they always securely encrypt any ePHI before it is transmitted over the network.

- **Authentication (ENV+CFG):** Administrative access to your Continuity Cloud node is controlled by a username and password. After you first gain access to the Continuity Cloud node, use the Windows control panel to change the password to a new password that is only known to you and is strong & unique. You must ensure that access to any VMs/applications running within the Continuity Cloud themselves are protected by appropriate authentication controls pursuant to the relevant requirements of HIPAA & HITECH.

- **Access Control:** Your Continuity Cloud credentials provide you with administrative management access over your Continuity Cloud node and any VMs running within it. Such management-level services are only accessible to an authenticated administrator of the Continuity Cloud node.

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

  - **(ENV):** Any VMs/applications you run within the Continuity Cloud must have suitable access controls to prevent unauthorized access to ePHI stored on top of the Continuity Cloud.

- **Audit Logging:**
  - **(ENV):** You must keep an audit trail anytime account credentials or any encryption keys are disclosed.

  - **(ENV):** Your environment must keep an appropriate audit log of all access to ePHI data that is contained within VMs/applications that you are running within the Continuity Cloud.

# BDR for Veeam: Minimum Security Baseline Guidelines

eFolder BDR for Veeam provides local, cross-site and cloud backup of virtual machine data. Data is encrypted in-transit and at-rest, using an encryption key is configured in the Veeam software and not known to eFolder. All data access is authenticated, and then 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 eFolder 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:** When properly configured, 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.

  - **Enable Veeam Encryption (CFG):** You must choose to enable encrypted backups within the Veeam software on the Veeam backup server. Use encryption for all backups and include encryption of backup jobs and target disks for drive seeding.

  - **Veeam Encryption Key (CFG):** You must configure Veeam with an encryption key that is known only to the organization that is authorized to access the ePHI. You must choose an encryption passphrase that will generate a sufficiently strong encryption key that meets or exceeds HIPAA requirements. You must protect this encryption key to prevent unauthorized disclosure.

- **Data Encryption in Transit (CFG):** All communications must be configured to be encrypted when in transit over the network to the eFolder cloud using the TLS protocol (SSL). To ensure protection from man in the middle attacks SSL must be chosen and the eFolder thumbprint must be verified when configuring eFolder as a service provider. Additionally, When configuring a server, NBDSSL must be chosen in the advanced section of the transport modes window (this is not the default option).

- **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 passphrase.

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

- **Audit Logging:** eFolder preserves an audit log of all data backed up to the cloud, data restores from the cloud, and configuration changes of the VEEAM agent, 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 Veeam agent that is responsible for sending data to the eFolder must be configured to encrypt at-rest data, stored to a "seed device". That device can then be shipped to eFolder in order. Make sure that you do not store your encryption pass phrase on the physical media, or is otherwise contained within the package that is shipped to eFolder. Follow all current seeding procedures described in the eFolder support knowledgebase. This is critical to ensuring HIPAA compliance of seed drives.

## Conclusion

eFolder 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 eFolder, 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. eFolder 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.

**Corporate Headquarters**
2340 Perimeter Park Drive, Suite 100, Atlanta, GA 30341 ▪ 678-888-0700 ▪ www.efolder.net ▪ sales@efolder.net