

eFolder considers security and compliance to be a critical part of our partnership with you. An example of our ongoing efforts is our ability to sign Business Associate Agreements (BAA) with respect to HIPAA compliance for additional eFolder services.

The following overview is intended to provide answers to commonly asked questions about eFolder's HIPAA compliance status. Please refer to our HIPAA Compliance Whitepaper (in the partner center) or email your account manager for further details.

Will eFolder sign a BAA?

Yes. eFolder will sign a BAA for certain eFolder services that are considered eligible for HIPAA compliance.

Will having a signed BAA from eFolder automatically make my client and/or me HIPAA compliant?

No. eFolder partners that offer a product or service to a HIPAA Covered Entity or another HIPAA Business Associate (BA) and are handling Protected Health Information (PHI) must sign a HIPAA Business Associate Agreement (BAA) with the customer. Having a signed BAA from eFolder does not make the BA or client HIPAA compliant by itself. Partners and their clients are responsible for their own compliance, and should work with their own legal counsel and/or auditors to ensure that they are properly complying with HIPAA.

Which eFolder services are eligible for HIPAA compliance?

- Anchor
- Backup for Files
- BDR for Acronis
- BDR for AppAssure (V5)
- BDR for ShadowProtect
- BDR for Veeam
- Continuity Cloud

Why is having a signed BAA important to me as a service provider?

Partners need to identify if they have clients that are considered Covered Entities under HIPAA. If their clients do qualify, then that client will need to have all Business Associates (BA) that they work with (that have access to electronic protected health information, also known as ePHI) sign a BAA. eFolder will sign a BAA with you in our role in providing cloud services to your organization and in turn your clients.

Will using eFolder services automatically make me HIPAA compliant?

No. There are many tasks and responsibilities that must be looked at to become HIPAA compliant. Having a signed BAA from eFolder is a necessary but not sufficient step for you to be HIPAA compliant. For more information please see <http://www.hhs.gov/ocr/privacy/> or speak to a HIPAA certified professional.

How do eFolder services work into my HIPAA offerings to my clients?

When working with a Covered Entity, a partner must also become HIPAA compliant to sign BAAs. Working with vendors like eFolder facilitates this process by ensuring that the tools you offer are safe and secure, and can be used in such a way that allows you to become or remain HIPAA compliant.

Where do I find more information about HIPAA HITECH and Final HIPAA Omnibus rule?

Please refer to our HIPAA Guidance Whitepaper for further details. Additionally, we recommend finding a reputable consulting firm or law firm that specializes in HIPAA compliance to assist you in your efforts to become or remain HIPAA compliant. Government websites such as <http://www.hhs.gov/ocr/privacy/> can also act as a reference.

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. The following indicates which services have been reviewed and are determined to be eligible for use in a HIPAA compliant environment, provided that they are configured and used properly. It is the responsibility of the partner or end-user organization to ensure that any eFolder services are configured and used in a manner that will cause the organization to be compliant with HIPAA. Please refer to the eFolder HIPAA Compliance Whitepaper for further guidance.

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

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.