WHITEPAPER

Guide to HIPAA Compliant Cloud Backup

For healthcare organizations, compliance is a major concern when deciding what to look for in a backup solution and cloud services. In this whitepaper, we will provide an overview of HIPAA basic principles, explain why the HIPAA regulation applies to cloud backup and discuss HIPAA-related backup requirements. We will also show how to create a HIPAA-compliant backup using MSP360 Backup software.

Table of Contents

HIPAA in a Nutshell

HIPAA stands for Health Insurance Portability and Accountability Act of 1996. It is a regulation for protecting personal medical data. HIPAA states that this data should be protected by any organization that has access to it.

HIPAA has a set of rules and terms, which should be carefully reviewed by anyone who is about to manage medical data. That includes not just healthcare businesses themselves, but also MSPs who provide services for healthcare businesses. Further down in the whitepaper you will find a breakdown of the main terms and rules of HIPAA, as well as a summary of requirements for HIPAA-compliant backup and recovery.

Main Terms and Rules

Legislation

HIPAA

The Health Insurance Portability and Accountability Act of 1996, which requires healthcare organizations to provide privacy and security for personal health information.

HITECH Act

- The Health Information Technology for Economic and Clinical Health Act, which extended HIPAA requirements (including civil and criminal penalties) to apply to business associates of covered entities (i.e., service providers of healthcare organizations).
- It also added a requirement to report data breaches that affect 500 or more individuals to the U.S. Department of Health and Human Services, the news media, and to the people affected by the data breaches.

HIPAA Main Rules

Privacy Rule

- Requires that organizations protect the privacy of personal health information in any form, whether electronic, paper, or oral.

Security Rule

- Requires ensuring the confidentiality, integrity, and security of health information that is held or transferred in electronic form.

Breach Notification Rule

- Requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Terms

Protected Health Information (PHI)

- Personal health information in any form, whether electronic, paper, or oral; must be protected as required by the HIPAA Privacy Rule.

Electronic Protected Health Information (ePHI)

- Personal health information that is held or transferred in electronic form; must be protected as required by the HIPAA Security Rule.

Covered entities

- Organizations that handle PHI and must protect it according to HIPAA compliance. Examples of such organizations include healthcare plans, healthcare clearinghouses, and healthcare providers that conduct certain healthcare transactions electronically.

Business Associate (BA)

- Any service provider (of a covered entity) that has access to PHI. The BA must comply with HIPAA and secure PHI in the same way as covered entities must.

Business Associate Agreement (BAA)

- Also known as a business associate contract, this is a written agreement that should be established between a covered entity and its BA to ensure that the BA will appropriately safeguard PHI.

Responsible Organizations

HHS

- The U.S. Department of Health and Human Services, which administers the HIPAA program, among other programs.

OCR

- The Department of Health and Human Services's Office of Civil Rights (OCR), responsible for HIPAA enforcement.

HIPAA violations are expensive. In 2018, OCR settled 10 cases and secured one judgment, which together totaled $28.7 million.

Cloud Services and HIPAA

Since a business associate is any service provider that creates, receives, maintains, or transmits ePHI, a cloud service provider (CSP) used by a healthcare organization falls into this category and therefore must follow HIPAA guidelines.

This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data. Lacking an encryption key does not exempt a CSP from business associate status and the associated obligations under HIPAA rules.

HIPAA-Compliant Cloud Storage Providers

There is no HIPAA certification, and the HHS makes no recommendations regarding specific cloud storage providers for HIPAA. However, to be HIPAA-compliant, cloud provider as a business associate of a covered entity (or as a business associate of another business associate) must enter into a HIPAA-compliant business associate agreement (BAA) and meet both:

- the terms of the BAA
- the applicable requirements of the HIPAA Rules.

BAA establishes the permitted and required uses and disclosures of ePHI by the business associate. It requires the business associate to safeguard the ePHI appropriately. OCR has created guidance on the elements of BAAs.

A Service Level Agreement (SLA) is commonly used to address more specific business expectations between the CSP and its customer, which also may be relevant to HIPAA compliance. For example, SLAs can include provisions that address such HIPAA concerns as:

- System availability and reliability
- Backup and data recovery (e.g., as necessary to be able to respond to a ransomware attack or other emergency situation)
- Manner in which data will be returned to the customer after service use termination
- Security responsibility
- Use, retention and disclosure limitations.

HHS published a special Guidance on HIPAA & Cloud Computing with the key questions and answers to assist HIPAA-regulated customers of cloud storage providers, and the providers themselves, in understanding their responsibilities under the HIPAA Rules.

HIPAA-Compliant Relationships Between Parties

Under HIPAA, compliance responsibility "flows" from the top down. If you are an MSP providing IT services for a hospital, you are below this hospital, and any vendors or subcontractors you work with are below you. A series of two-party agreements are required down the line from the hospital to you and from you to your subcontractors.

The hospital is responsible to the patients for protecting their personal information. You as an MSP commit to the hospital that you will protect the confidential information and sign a BAA with the hospital. Your subcontractors (for example a cloud service provider) commit to you that they will protect the patients' information as well and sign a BAA with you.

HIPAA Requirements for Data Backup and Recovery

HIPAA Security Rule includes three types of safeguards required for compliance: **administrative, physical,** and **technical**. For each of these types, HIPAA includes different security standards, and for each standard, it identifies both "required" and "addressable" implementation specifications.

"Required" specifications must be adopted and administered as dictated by the HIPAA Rules. "Addressable" specifications are more flexible. Individual covered entities and BAs can analyze their specific situation and determine the best way to implement addressable specifications.

The table below summarizes HIPAA requirements directly related to backup and recovery.

Administrative Safeguards

- **Standard:** Contingency Plan
- **Goal:** Develop processes that enable the organization to respond to an emergency or other occurrence that threatens the integrity or availability of ePHI.

Section	Implementation Specification, (R)=Required, (A)=Addressable	Action needed
§ 164.308(a)(7)(ii)(A)	Data Backup Plan (R)	Develop a plan for backing up all ePHI.
§ 164.308(a)(7)(ii)(B)	Disaster Recovery Plan (R)	Develop a set of procedures to ensure protection of PHI in the event of a disaster.
§ 164.308(a)(7)(ii)(D)	Testing and Revision Procedures (A)	Engage in periodic testing and revision of the contingency plan.
§ 164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis (A)	Determine how important each data application, that stores, maintains or transmits ePHI, is to patient care or business needs. Prioritize for data backup, disaster recovery and/or emergency operations plans.

Physical Safeguards

- **Standard:** Facility Access Controls
- **Goal:** Have policies and procedures to limit access to the computer systems where ePHI is maintained.

Section	Implementation Specification, (R)=Required, (A)=Addressable	Action needed
§ 164.310(a)(2)(i)	Contingency Operations (A)	Establish and implement procedures that allow facility access in support of roestoration of lost data under the disaster recovery plan and emergency moode operations plan in the event of an emergency.

- Standard: Device and Media Controls
- Goal: Ensure proper handling of electronic media including receipt, removal, backup, storage, reuse, disposal and accountability.

Section	Implementation Specification, (R)=Required, (A)=Addressable	Action needed
§ 164.310(d)(2)(iv)	Data Backup and Storage (A)	Create a retrievable, exact copy of ePHI before moving equipment that contains ePHI to protect its availability.

Technical Safeguards

- **Standard:** Access Control
- **Goal:** Allow access to ePHI only to authorized users and software.

Section	Implementation Specification, (R)=Required, (A)=Addressable	Action needed
§ 164.312(a)(2)(iv)	Encryption and Decryption (A)	Implement a mechanism to encrypt and decrypt ePHI in order to protect it from being accessed and viewed by unauthorized users.

- **Standard:** Transmission Security
- **Goal:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted.

Section	Implementation Specification, (R)=Required, (A)=Addressable	Action needed
§ 164.312(e)(2)(i)	Integrity Controls (A)	Ensure that ePHI is not improperly modified during transmission.
§ 164.312(e)(2)(ii)	Encryption (A)	Encrypt ePHI when it is being transmitted.

HIPAA Encryption Requirement

Although some implementation specifications are listed as "addressable", that doesn't mean they are optional.

For example, the HIPAA encryption requirement is marked as "Addressable," but note how HHS answers here whether encryption is mandatory:

> **"If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate."**
> **You don't have to encrypt data, but you'd better do it.**

This means you don't "have to" encrypt, but you'd better be prepared to demonstrate, in writing, why you believe that you don't have to. Then, in the event of an audit, the Office for Civil Rights (OCR) will review your documentation and determine whether or not they agree with you.

There probably are very few scenarios where encryption "is not reasonable and appropriate," or where there is an easier alternative to protect health information, so it always makes sense to implement it. Also, breached data is not considered unsecured if the PHI "is rendered unusable, unreadable or indecipherable to unauthorized individuals." Encrypted data fits this definition.

Summary of Requirements for HIPAA-Compliant Backup and Recovery

To summarize the practical part of related to backup and recovery, HIPAA standards require that you:

- Develop a PHI backup plan and disaster recovery plan to follow HIPAA Administrative Safeguards.

This should be done according to the priorities set for data applications that handle ePHI, depending on how important they are for patient care and business needs.

- Protect your backups of ePHI from unauthorized access, disclosure, alteration, and destruction to follow HIPAA Technical Safeguards.

Although encryption is not formally "required," it's necessary to use it in order to protect important health information.

- Back up PHI to multiple locations to protect its availability, as HIPAA Physical Safeguards suggest.

One of the most effective ways to ensure your data is protected from physical damage is to follow the 3-2-1 backup strategy.

HIPAA-Compliant Backup Solution

On its own, no software can make you HIPAA-compliant. However, MSP360 Backup can help you to meet HIPAA requirements and make it easy to follow your HIPAA-compliant backup and disaster recovery plans by providing the following features:

- **End-to-End Encryption**

Secure data in transit and at rest with AES-256 encryption. Be sure that all your PHI data is protected.

- **Hybrid Backup**

Configure backup to local and cloud storage in a single backup plan for your convenience. Easily follow the 3-2-1 backup strategy.

- **Data Archiving**

Since retention requirements for HIPAA vary based on the type of record, MSP360 Backup lets you store as many versions as you need for as long as you need with its flexible retention settings.

Thinking Beyond HIPAA for Backup

MSP360 Backup provides other features to give you a powerful backup and recovery solution:

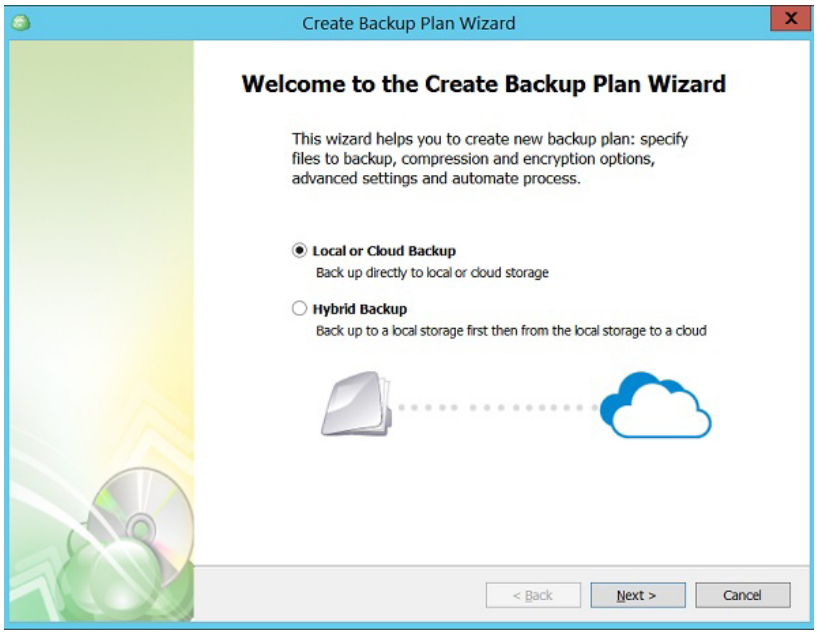
- Protect entire servers with system image backup
- Protect files with file and folder backup
- VMware, Hyper-V and Amazon EC2 snapshot support
- Intelligent incremental backups for best performance
- Microsoft VSS support for uninterrupted backups
- Backup compression to reduce storage costs
- Bare-metal recovery for extra protection in the event of a major disaster

How to Perform a Backup using MSP360 Backup

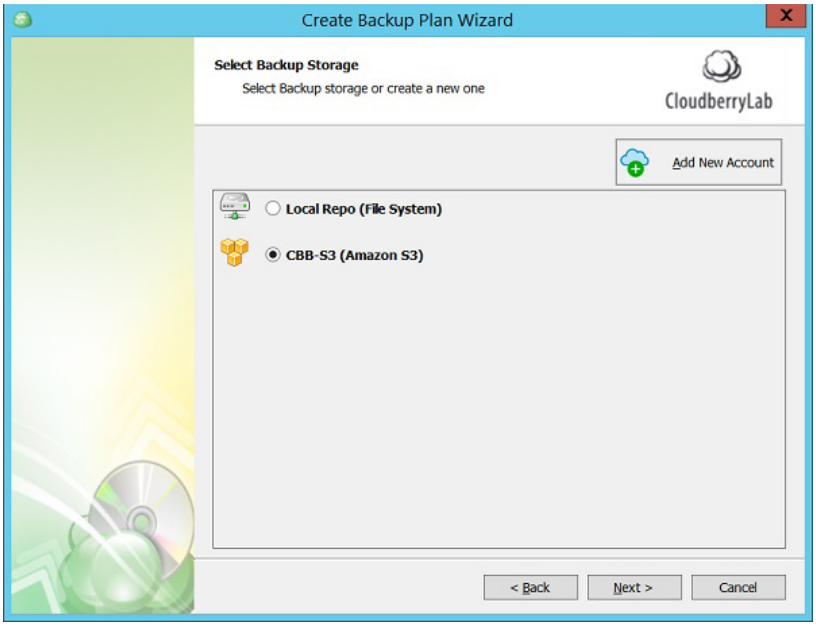
Let's suppose that patient medical records are on-site, in folder D:\data.

We will now set up regular data backup in MSP360 Backup. For this example, we will use Amazon S3 cloud storage. For more info on how to use Amazon S3 as a backup storage destination check out our guide.

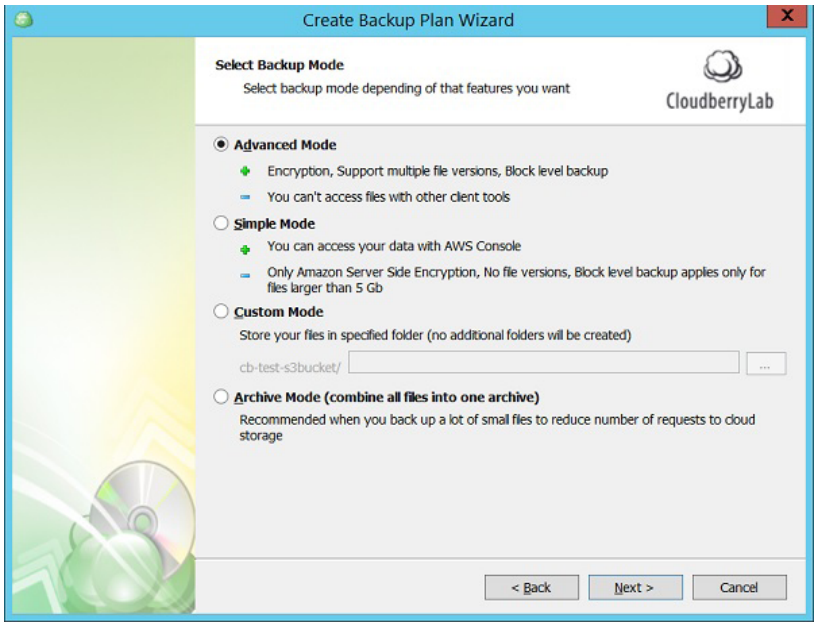
1. Select Local to Cloud in the main window. You can select either **Local or Cloud Backup** or **Hybrid backup**. Hybrid backup is a feature that allows you to perform local and cloud backup in one take.



2. Select the required cloud storage account (you can add a new provider in Add New Account on the same tab):



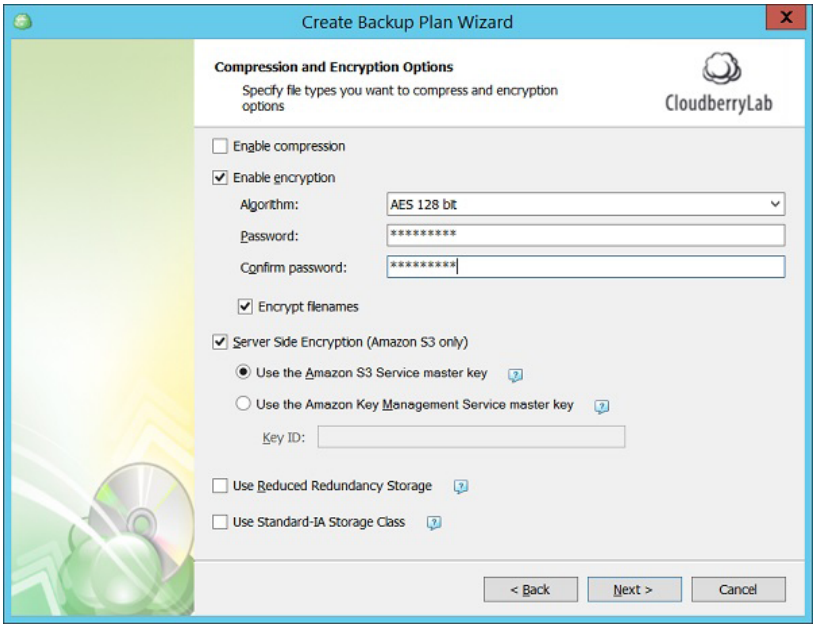
3. Enter the name of the backup plan and select Advanced Mode – this will allow you to choose encryption settings, both for Amazon and MSP360 Backup.



4. To prevent backup issues related to opened files and/or permissions, you should use VSS and copy NTFS permissions.

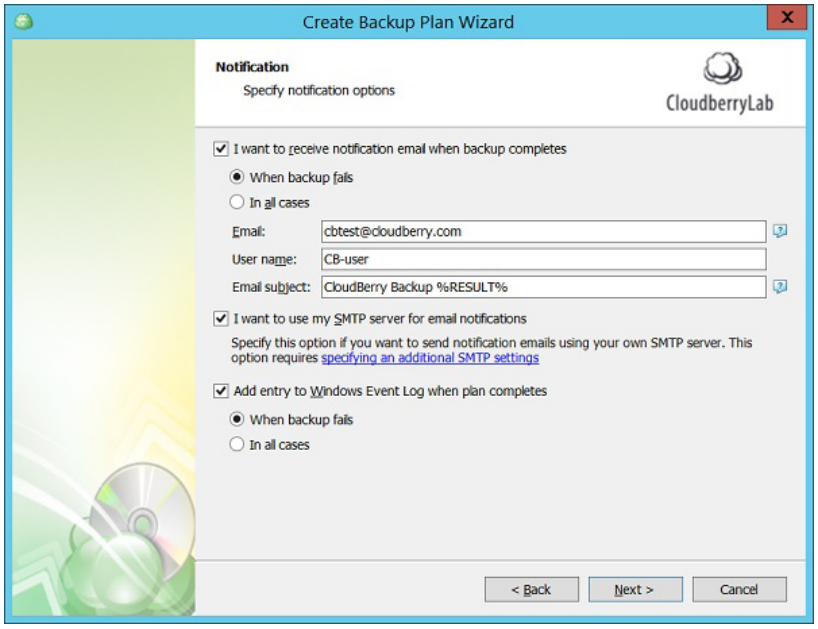
5. Choose the data to back up. If necessary, set exception filters for any files or folders which you do not need to back up..

6. Set the backup encryption. You can use MSP360 Backup encryption instead of AWS encryption – backups, in this case, data will be encrypted before the transfer to the cloud. Since only your company knows the encryption password, data cannot be decrypted without this password. However, it's acceptable to use MSP360 encryption with AWS Server-Side Encryption to add a second layer of protection.



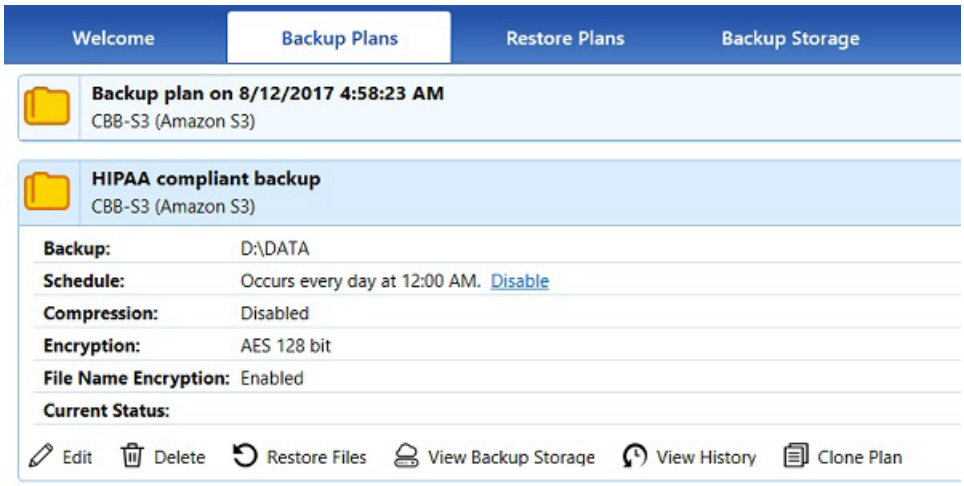
7. Set up the policy for archive deletion, archiving schedule(s), and the start of programs and scripts, pre- and post-backup.

8. Set up email notifications for successful or unsuccessful backups completion. Windows Event Logging can also be used to generate notifications by your central monitoring system since these systems often monitor the Windows System Logs.



9. Review the backup plan parameters to complete the setup process.

You can find the newly created HIPAA-compliant backup plan on the Backup Plans tab:



Patient medical records are now protected from hardware failure and unauthorized access thanks to AWS and MSP360 Backup. You can back up SQL Server and Exchange databases in a similar way.

Try to create a backup copy of data using the free trial version of MSP360 Backup.