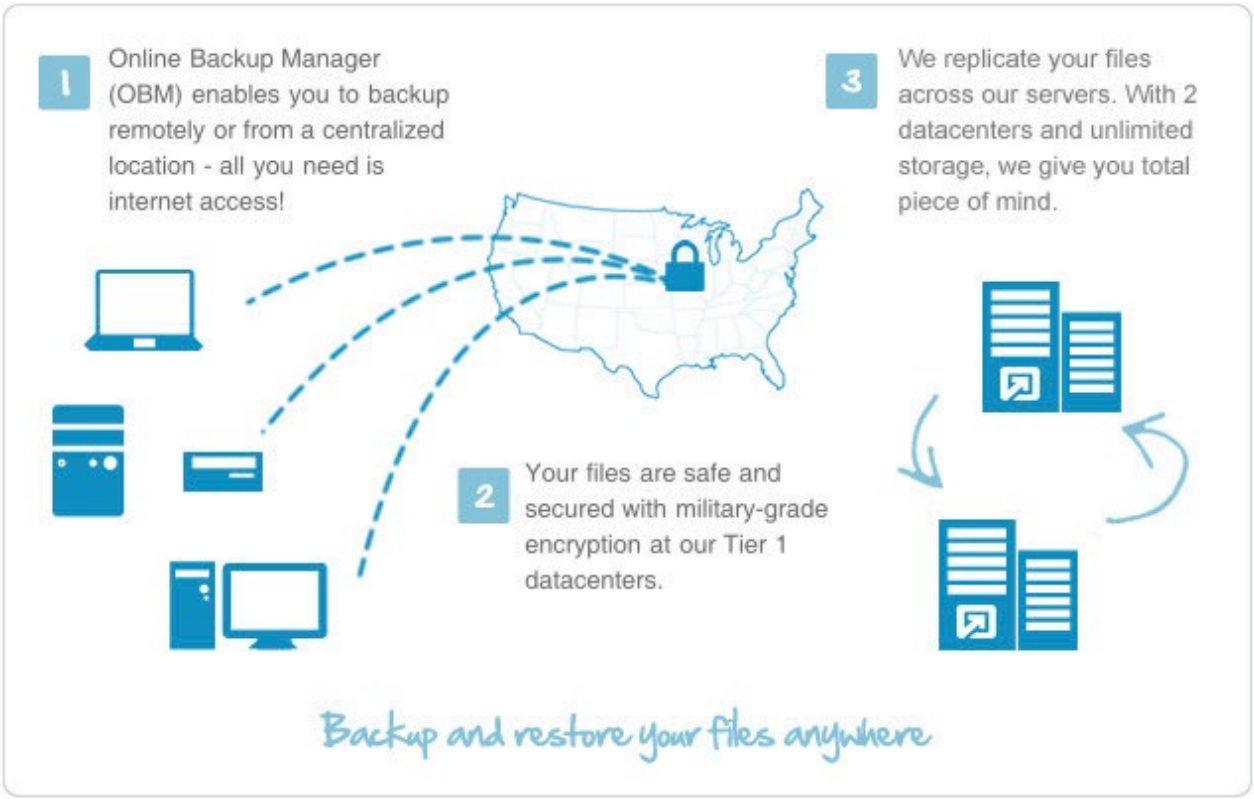

1. Secure 128-Bit SSL Communication

All communications between Offsite Backup Server and your computer are transported in a 128-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (internet), eavesdroppers have no knowledge of what has been exchanged.

2. Backups Are Securely Encrypted

All of your files are first zipped and encrypted with a user-defined encrypting key before they are sent to the Offsite Backup Server. To all people but you, your files stored on the Offsite Backup Server are no more than some trashed files with random content.

3. We Don't Keep Your Encryption Key

The encryption key used to encrypt your files resides only on your computer and is known only to you. It is never transmitted anywhere across the network. If this key is lost, all backup files can never be recovered. Therefore, although we have access to all files you stored on our Backup Server, we have no knowledge of the content of the files you stored.

VERY IMPORTANT: Please make sure you write down your encryption key and keep it in a safe place where it will never be forgotten. Otherwise, you will never be able to recover your backup files.

4. The Best Encryption Algorithm Is Used

Currently, the algorithm that we use to encrypt your files is 128-bit Twofish. It is a block cipher designed by Counterpane Labs. It was also one of the five Advanced Encryption Standard (AES) finalists chosen by National Institute of Standard and Technology (NIST). It subjects to frequent public reviews but no known attack against this algorithm has been reported.

5. It Would Require 8.77 x 1,017 Years To Crack Our 128-Bit Encryption

A 128-bit key size has 2,128 or around 3.4 x 1,038 possible combinations. Even if you have the world's best super computer, ASCI White, SP Power3 375 MHz manufactured by IBM as of November 2000, it would take 8.77 x 1,017 years to test all combinations. Assuming you have this super computer, the ASCI White, SP Power3 375 MHz has 8,192 processors which totals a capability of 12.3 teraflops (trillions of operations/second), available to you. Also it just needs one computer operation to test a possible combination (which is already faster than what it can do). To use brute force attack (checking all combinations) on this encryption algorithm. It would take:

3.4 x 1,038 possible combinations / 12.3 x 1,012 seconds (approximately 2.76 x 1,025 seconds)

(i.e. 876530835323573935 years or 8.77 x 1,017 years) to successfully try all combinations. Let alone the ASCI White cannot process as fast as what is described here. You can be sure that your data stored on our server is 100% secure!

6. Restricted Access To Your Data By IP Address

You can also restrict access to your backup files from the set of IP addresses you have defined. If someone tries to access your data from an IP address not on your defined list, their access will be denied. This additional security ensures that backup files are not open to all locations, even if the username and password are known.

How We Help You With HIPAA

We knows our healthcare clients have HIPAA-compliance responsibilities, and we are here to help. Our systems and services are designed for absolute security and privacy, so we integrate perfectly with your HIPAA compliance efforts, including HIPAA online backup.

The HIPAA Privacy Rule

HIPAA's Privacy Rule, among other things, sets minimum standards for the protection of confidential patient information, called PHI or "Protected Health Information". PHI must be protected against all "reasonably anticipated" threats, physical and electronic. For the average health care provider or health plan, the Privacy Rule requires certain activities, such as:

- Providing information to patients about their privacy rights and how their information can be used.
- Adopting clear privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

We are the premier online data backup provider for healthcare entities utilizing best practice data-serving technology and security software. This means that the health data you backup online and store with Online Backup Manager is protected to standards that meet or exceed HIPAA's requirements.

Currently, the algorithm that we are using to encrypt your files is 128-bit Twofish. It is a block cipher designed by Counterpane Labs. It was also one of the five Advanced Encryption Standard (AES) finalists chosen by National Institute of Standard and Technology (NIST). It has been subjected to frequent public reviews but no known attack against this algorithm has been reported. It would require 8.77 x 1017 years to crack our 128-bit encryption!

The Bottom Line

Your patients' PHI remains safe, secure, and *private* with HIPAA-compliant Online Backup Manager.

The HIPAA Security Rule

HIPAA's Security Rule establishes a new term: "ePHI", or "Electronic Protected Health Information". ePHI is any PHI that is in electronic or digital form. With the increasing use of computers and networks, PHI is increasingly becoming ePHI. From patient tracking, to testing and diagnosis, to treatment and care, the medical community is creating mountains of electronic health information that has to be protected and Online Backup Manager is the best data backup and protection solution available.

The Security Rule (section 164) specifically requires, among other things, that the following listed safeguards be used to protect ePHI:

1. Data Backup Plan – 164.308(a)(7)
2. Disaster Recovery Plan – 164.308(a)(7)
3. Emergency Mode Operations Plan – 164.308(a)(7)
4. Emergency Access Procedures – 164.312(a)(1)
5. Data Backup and Storage – 164.310(d)(1)
6. Contingency Operations – 164.310(a)(1)
7. Encryption & Decryption – 164.312(a)(1) and 164.312(e)(1)

For each of these security requirements, OBM supports you in your compliance efforts:

1. Data Backup Plan – Leading IT experts agree that backing up critical data frequently and offsite is one of the best ways to protect your business, and reduce your risk from data losses. Your data backup plan should include OBM, the most secure, cost-effective choice for data backup.

2. Disaster Recovery Plan – In an uncertain world, a disaster recovery plan is worth its weight in gold, especially where critical patient data is involved. After a disaster, secure and immediate access to your data is crucial element of the disaster recovery process. If your own servers and networks are down or damaged, rely on Online Backup Manager to keep your data safe and accessible whenever and wherever you need it.

3. Emergency Mode Operations Plan – Some disasters and emergencies last longer than others. If you have to execute your Emergency Mode Ops Plan, it means you're dealing with an extended outage of your normal operations. In such a scenario, OBM is your most reliable and secure data resource. You can run your operations from almost anywhere as long as you have your data. And nobody provides safer, more secure storage and access to your data than Online Backup Manager.

4. Emergency Access Procedures – Emergency access may be needed for any number of reasons: a fire or flood in your building; a sudden legal challenge; or the death of a key IT employee. Just as with Emergency Mode Operations and Disaster Recovery, We facilitates secure, 24/7 access to your data whenever and wherever you need it.

5. Data Backup and Storage – Threats to your data can come from many directions: human error; theft or sabotage; device failures; etc. That's why an essential requirement of HIPAA's Security Rule is data backup and storage. Don't make the mistake of storing and backing up you data on your own site. Experts universally agree that offsite storage, done right, is more secure than onsite storage, and reduces your risk of data loss. With Online Backup Manager, you can restore your data in mere seconds, all the way back to when you first started with our Online Backup Manager, from any day, on any file.

6. Contingency Operations – As with Emergency Mode Operations, Contingency Operations require you to keep working under difficult circumstances. When your operating environment is uncertain or in flux, OBM is your rock-solid data resource, protecting your digital assets from hackers, natural disasters, or just a simple computer crash every day of the year.

7. Encryption & Decryption – Because it protects data from prying eyes, encryption and decryption were made an essential HIPAA requirement. Online Backup Manager's process compresses and encrypts prior to transmitting over a secure internet channel (SSL), so rest assured your data is safe. Our 128-bit SSL encryption is 100% guaranteed.

Our Online Backup Manager helps you fulfill your HIPAA Compliance Requirements with its online backup. Like HIPAA Compliance itself, protecting your critical data is a huge responsibility. Because we built our systems and services for specifically for security and privacy, HIPAA Covered Entities can rely on our Online Backup Manager to blend seamlessly with their HIPAA compliance efforts.

OBM is a premier online data backup provider for HIPAA Covered Entities, utilizing best practice data-serving technology and security software. Without any installation fees or additional equipment to purchase, you can start protecting your data right now!

Technology Business Solutions

Online Backup Manager

50 GB	$15 Month
100 GB	$25 Month
250 GB	$50 Month
500 GB	$100 Month

Replicated Data Storage	✔
Windows	✔
Mac	✔
Linux	✔
Unix	✔
Exchange	✔
SQL	✔
MYSQL	✔
VMWARE *add. VM cost	✔
HYPER-V *add. VM cost	✔
LOTUS NOTES / DOMINO	✔
ORACLE	✔