

## HIPAA Compliance

HIPAA has enacted several mandates to improve the access and portability of patient health records while maintaining strict privacy and security. A critical aspect of the HIPAA privacy ruling is Data Protection, requiring compliant backup methodologies to ensure the security and confidentiality of patient records. Health care providers who engage in electronic transactions must observe privacy safeguards to restrict the use and disclosure of individually identifiable health information.

**Off Site On Line Backup supports HIPAA compliance through automated off-site data protection with on-demand recovery, while ensuring strict data security and confidentiality.**

## Requirements

### Restrict Unauthorized Access

Patient record confidentiality is critical. Any electronic data transfer and storage must be adequately protected and secure from all unauthorized access.

### Contingency Plan

Organizations are required to have a contingency plan to continue operations in the event of data loss. This contingency plan MUST include details concerning the data backup and recovery process, who handles the backup media, the media rotation process, where the media is stored off-site, how quickly it can be retrieved in the event of a disaster, and all other aspects associated with data backups, protection, security, storage, and recovery.

Data loss can result in further losses of productivity, patients/customers, and revenue. In many cases significant data loss will result in lost business. Fortunately, the damaging impact of data loss can be negated with a qualified data protection solution as part of your contingency plan.

## Data Protection Options

### Tape Drives

- Initial investment starts at \$2,000 for the drive and backup software. Consider this a semi-annual expense since drives will wear out.
- A rotating backup methodology uses a minimum of 19 tapes per year -averaging another \$800 per year for tape storage media.
- Tapes have a limited shelf life. Due to tape costs and media rotation hassles, it is common to resort to taping over and over on the same tape, only to discover that the tape has worn out, rendering the backups unusable.
- Off-site storage is required. Convenient storage and expedited retrieval is necessary for emergency situations.
- Tape storage space is limited and not conducive to automated, unattended backups.

### Removable Storage Drives

- These devices require a high entry price for a reliable system.
- Off-site storage is required. Convenient storage and expedited retrieval is necessary for emergency situations.
- Storage capacity limitations make automated and unattended backups impractical.

### External Disc Media (CDs, DVDs)

Due to their low price point and readily available drives, rewritable CDs (CD-RW) and DVDs have become a popular backup media. However, you should note that:

- CDs have less storage capacity than tapes, making automated and unattended backups impractical.
- DVDs have a larger storage capacity than CDs, but are still limited.
- Off-site storage is required. Convenient storage and expedited retrieval is

- necessary for emergency situations.
- Limited shelf life is a definite concern.

Since external backup storage media (Zip drives, CDs, DVDs, Tapes, Flash drives, external hard drives, etc.) can be easily stolen, support limited data sizes, often utilize no or minimal encryption security and must be transported to/from off-site storage facilities, they seldom represent adequate data protection solutions for HIPAA compliance.

#### **Off Site Online Backup Services**

Online backup services represent a fully-automated, secure, unlimited off-site storage facility for quality data backup operations.

- Fully automated data backups at secure off-site facilities.
- No hardware to buy or manage.
- No media to buy, rotate, catalog or store offsite.
- All data is encrypted for security.
- Data can be easily restored on-demand 24x7.
- Service costs can be low compared to external media.

#### **Off Site On Line Backup for HIPAA Compliance**

HIPAA compliant information systems require a combination of administrative procedures, physical safeguards and technical measures to protect patient information during storage and transmission across communication networks. As a significant part of your overall contingency plan, Off Site On Line Backup provides secure, automated data transmission and storage services for data backup and recovery.

#### **Off Site On Line Backup implements the following HIPAA compliant features:**

- Automated, unattended data backups with built-in notifications.
- Ultimate data security via 448-bit encryption – data is ALWAYS compressed and encrypted during transmission and storage.
- Data integrity controls with mutual authentication.
- Restricted password access – a secret encryption key can be specified for ultimate security, even Off Site On Line Backup can't get access your data.
- Off-site storage at highly-secured data centers.
- Data is mirrored to secondary secure facilities for ultimate data availability
- Extended storage is available (HIPAA requires storage for minimum 6 years).
- On-demand, exact copy data retrieval - 24x7x365.
- Optional monthly CD or DVD archives are available.

#### **Additionally:**

- No cost or hassles with external devices, media, or offsite storage.
- US company with the lowest subscription rates in the industry.

HIPAA privacy rules provide Off Site On Line Backup and its affiliates with "business associate" rights to limited use and disclosure of the information. Off Site On Line Backup never discloses data unless required by law. Off Site On Line Backup does not access any portion of the backup data unless authorized for customer support purposes. Off Site On Line Backup can be fully prevented from data access by use of the client-side secret encryption key.

Please visit the [Office for Civil Rights - HIPAA](#) website for more information about the national standards to protect the privacy of personal health information.

## **HIPAA Overview**

HIPAA consists of five parts:

- Title 1 - Health Insurance Portability - helps workers maintain insurance coverage when they change jobs
- Title 2 - Administrative Simplification - standardizes electronic health care-related transactions, and the privacy and security of health information
- Title 3 - Medical Savings Accounts & Health Insurance Tax Deductions
- Title 4 - Enforcement of Group Health Plan provisions
- Title 5 - Revenue Offset Provisions

Fortunately, four of the five parts of HIPAA have no bearing on Remote Backup. The one part that does apply is Title 2 - Administrative Simplification.

### **Administrative Simplification**

HIPAA Administrative Simplification consists of two areas. The first is commonly referred to as the Transactions and Code Sets Rule, although it also covers standardization of identifiers. This Rule requires standardization in all health-related electronic transactions, such as electronic transmission of insurance claims, verification of insurance, statements, explanations of benefits, remittance advice, etc. It is scheduled to take effect in October 2003.

Off Site On Line Backup is not a health-related transaction, and is therefore not covered under the Transactions and Code Sets Rule.

The second area of Administrative Simplification is made up of two Rules, the Privacy Rule and the Security Rule. Because these two rules are where the most confusion arises, we will examine them in some detail.

### **Privacy and Security**

Before the Privacy and Security Rules can be explained, we must understand what they are intended to protect. Both Rules are intended to safeguard any health-related information that can be traced to or used to identify an individual. Some examples of this type of information include name, address, Date of Birth, Social Security number, or any other identifier. This type of information is referred to as Protected Health Information, or PHI.

The Privacy Rule and Security Rule are intended to protect PHI in different ways. The Privacy Rule sets out limits on who can have access to PHI and for what purpose. The Security Rule regulates the Procedural, Physical and Technical means that are used to protect PHI.

### **Privacy**

The Privacy Rule places limits on the ways that PHI can be used and disclosed, and requires accounting of disclosures. But it is relevant at this point to review how Off Site On Line Backup works.

With Off Site On Line Backup solution, all information to be backed up is encrypted by the local client before being transmitted, using a key that is stored locally. Data is stored on the remote server in its encrypted form. Data can only be recovered by transmitting it back to the local client, which decrypts it, again using the locally-stored key. The most important feature of this arrangement is that while the data is stored on the remote server, it is encrypted and not in a readable format. The remote server does not have access to the key, and without the key, the data

cannot be converted to a readable format.

Off Site On Line Backup Services do not involve the use or disclosure of PHI. All back-up data is stored on the Remote Server in an encrypted form, and any access to PHI by a Off Site On Line Backup Service Provider would be incidental, if even possible. Off Site On Line Backup Service Providers are therefore not normally considered to be Business Associates, and are not covered by or required to be compliant with the HIPAA Administrative Simplification Privacy Rule.

## **Security**

The Security Rule is the one part of HIPAA that clearly applies to the type of services that Off Site On Line Backup offers. The Final Security Rule was published in February 2003, and became effective on April 21, 2003. Compliance with this Rule will be required by April 21, 2005.

The Security Rule legislates the means that should be used to protect PHI. It requires that covered entities have appropriate Administrative Procedures, Physical Safeguards, and Technical Safeguards to protect access to PHI.

Examples of appropriate safeguards include:

- Establishment of clear Access Control policies, procedures, and technology to restrict who has authorized access to PHI.
- Establishment of restricted and locked areas where PHI is stored.
- Establishment of appropriate Data Backup, Disaster Recovery, and Emergency Mode Operation planning.
- Establishment of technical security mechanisms such as encryption to protect data that is transmitted via a network.

### ***Off Site On Line Backup is compliant with the Final Security Rule.***

The Off Site On Line Backup client software contains all appropriate technical security mechanisms to protect the data that is transmitted to and from the Off Site On Line Backup Server.

Off Site On Line Backup can form a critical part of Data Backup, Disaster Recovery, and Emergency Mode Operations strategies by providing offsite backup that can be geographically distant from the client site to minimize the likelihood of data loss in a large-scale disaster. In the event of loss of the primary data center, data on a Off Site On Line Backup Server can easily be recovered from any replacement data center.

Covered entities will be required to comply with the HIPAA Administrative Simplification Security Rule by April 21, 2005. Remote Backup, as part of a comprehensive security plan, can be an important part of compliance strategy.