

Online Backup and Storage and HIPAA Compliance

Discussion and debate over how HIPAA dictates online backup and storage solutions has continued for the past five years. This paper gives the facts and innuendo surrounding the discussion.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was designed to:

1. Reduce the administrative costs of healthcare
2. To promote the confidentiality and portability of patient records
3. To develop standards for consistency in the health care industry
4. To provide an incentive for electronic communications



HIPAA applies to any health care provider, health plan and clearing house (collectively "Covered Entities") that electronically maintain or transmit health information pertaining to individuals. Covered Entities must have appropriate measures that address the physical, technical and administrative components of patient data (information) privacy.

With the exception of small health plans, all Covered Entities are required to have data security standards in place by April 21, 2005, when the Standards for the Security of Electronic Protected Health Information (the "**Security Rule**") of HIPAA went into effect for most health care providers. Small health plans were exempted until April 21, 2006.

The Security Rule requires health care providers to put in place certain administrative, physical and technical safeguards for electronic patient data. Among other things, Covered Entities will be required to have a *Data Backup Plan*, a *Disaster Recovery Plan*, and an *Emergency Mode Operation Plan*.

The HIPAA Security Rule

The Security Rule applies to electronic protected health information. This is protected health information either transmitted by electronic media or maintained in electronic media. Covered Entities that maintain or transmit protected health information are required by the Security Rule (see 45 C.F.R. §164.306) to:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information that 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 subpart E of this part.
4. Ensure compliance with this subpart by its workforce.

According to the HIPAA regulations, Covered Entities are allowed to use a flexible approach when implementing the above requirements. Specifically,

1. Covered Entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
2. In deciding which security measures to use, a covered entity must take into account the following factors:
 - i. The size, complexity, and capabilities of the covered entity
 - ii. The covered entity's technical infrastructure, hardware, and software security capabilities
 - iii. The costs of security measures
 - iv. The probability and criticality of potential risks to electronic protected health information

The Security Rule is further detailed through eighteen technical standards and thirty six implementation specifications. These standards and specifications are classified into four categories: administrative safeguards, physical safeguards, technical safeguards and organizational requirements.

HIPAA Security Rule and Electronic Data Backup

A number of the Security Rule's standard and specifications apply to the backup and safekeeping of electronic data. Covered Entities must have a contingency plan and:

“Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information (Administrative Safeguards - §164.308(a)(7)(i)).”

This contingency plan must be implemented as follows:

1. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
2. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.
3. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Covered Entities must also have certain physical safeguards, such as facility access controls. They must:

“Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed (Physical Safeguards - §164.310(a)(1)).”

The contingency operations should establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency (§164.310(a)(2)(i)).

In addition, Covered Entities must implement certain technical safeguards (§164.312) to, among other things:

- Limit access to and electronic protected health information.
- Encrypt and decrypt electronic protected health information.
- Put into place audit controls that record and examine activity in information systems that contain or use electronic protected health information
- Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

DataPreserve Online Backup and Storage Solution and HIPAA Compliance

DataPreserve Online Backup and Storage can help Covered Entities meet HIPAA compliance requirements, specifically those of the Security Rule.

DataPreserve Security and Encryption

All data, including patient and billing records, is encrypted before it leaves the user's computer(s) and is never accessible without the user's password. This password is

stored only on the user's system and is never transmitted over the Internet nor is it stored on the DataPreserve servers. Thus, only the user has access to the encrypted information, eliminating the threat of unauthorized access. Even DataPreserve cannot access the files or even read the filenames.

Each file is individually encrypted using Advanced Encryption Standard (AES) encryption technology. AES encryption was developed by the U.S. National Institute of Standards and Technology (NIST) and is now the state-of-the-art standard encryption technique for both commercial and government applications.

For added security, and to meet the Security Rule's transmission requirements, each encrypted file is then sent over the Internet via a secure channel using Secure Sockets Layer (SSL) technology. This is the same Internet transmission technology that is used for online banking and online credit card applications. As a result, data is encrypted twice. It is encrypted at all times using the AES encryption, and it is encrypted again while it is being sent over the Internet, to and from the DataPreserve servers.

Further, all user data is sent to and stored in our SAS-70 tier-4 data center. Tier-4 data centers have 24/7 onsite monitoring, advanced security technology such as biometric access controls, backup generators and redundant connections to the Internet.

DataPreserve Logging and Archiving

Each file that is backed up or restored, as well as additional information and statistics about backups is recorded in a log within the DataPreserve Online Backup and Storage software. This log, which can easily be searched, allows the user to verify that files were successfully backed up and help troubleshoot any issues that may be occurring. The user also has the option of receiving an automated email notification at the conclusion of each successful backup. Information about recent backups and total storage usage can also be viewed via the Internet, by logging on to the user's account.

Backing Up and Restoring with DataPreserve Online Backup and Storage

Backups and restores are automated, eliminating the need for manual data handling. Backups will begin automatically according to each backup set's backup schedule as long as the computer is on and functioning. Backups can also be initiated by the user at any time. Because backups run in the background of the system, they have little or no impact on the computer's performance or Internet connectivity.

Restoring files can be done in just a few clicks of the mouse. Using the DataPreserve software, the user simply clicks on the individual files or folders or revisions that he or she wants to retrieve. The file or files will then be downloaded to the user's computer, decrypted, uncompressed and then restored to their original location or another specified

location on the user's system. A password is required to restore any files, preventing unauthorized restores, as per the HIPAA Security Rule.

In the event of a complete system failure, a full recovery of the user's stored data can be initiated in minutes. This recovery can be done on any Windows based computer, and not just the computer from which the files were originally backed up. The user will download and reinstall the DataPreserve software, enter the username and Password. Once the software installation is completed, two clicks of the mouse will restore the file catalogue (the list of all of the files backed up) which will then give the user the ability to restore any and all files backed up.

More on HIPAA

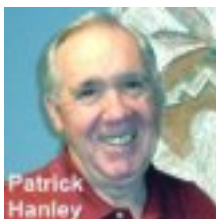
For more information on HIPAA compliance and data backup, DataPreserve recommends these resources:

- Summary of the HIPAA Privacy Rule www.hhs.gov/ocr/privacy/hipaa/understanding/summary/
- Updates on HIPAA www.hipaa.com

Please note that nothing in this White Paper is intended to constitute legal advice. For more information about HIPAA and compliance with HIPAA requirements please consult your legal counsel.

About the Author

Patrick Hanley is the General Manager of Field Operations for DataPreserve Inc. Mr.



Hanley's experience includes over thirty years in both the domestic and international IT Services sector. Mr. Hanley joined DataPreserve in 2004 and he continues to provide leadership on internal and external relationship management of the channel, customers, and other business partners. During that time he has worked with hundreds of technology professionals and thousands of clients sharing his in-depth knowledge of online backup and storage best practices to meet statutory and other business requirements.

He can be reached at 480.422.1583 or phanley@datapreserve.com.