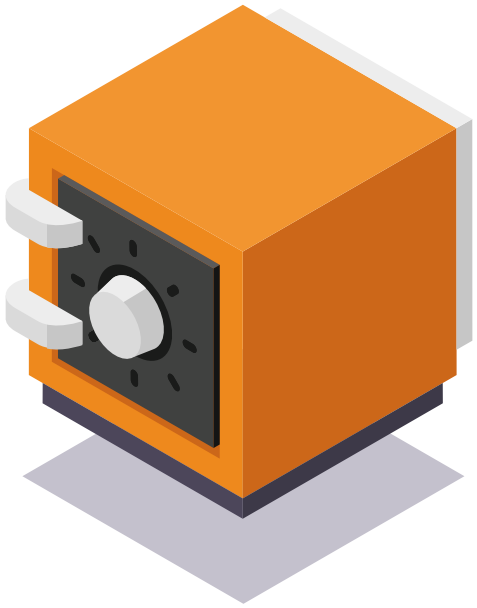
KeepItSafe®



HIPAA
COMPLIANT DATA BACKUP AND DISASTER RECOVERY

Learn more about how KeepItSafe can help to reduce costs, save time, and provide compliance for online backup, disaster recovery-as-a-Service, mobile data protection, and cloud SaaS backup — contact us today.

888 965 9988

www.keepitsafe.com

sales@keepitsafe.com

TABLE OF CONTENTS

Overview

The federal government passed the original Health Insurance Portability and Accountability Act (HIPAA) in 1996 as a law designed to:

1. Protect workers from losing their medical insurance coverage if they change or lose their jobs.
2. Reduce the administrative costs of healthcare, specifically by promoting electronic record keeping.
3. Increase the security and portability of patient records.
4. Develop standards for consistency in the healthcare industry.

HIPAA applies to all healthcare providers, health plans and clearing houses, known collectively as "covered entities," that electronically maintain or transmit health information of individuals. Covered entities must have appropriate measures that address the physical, technical, and administrative components of patient data (information) privacy.

The Security Rule of HIPAA requires healthcare providers to put in place certain administrative, physical, and technical safeguards for protected patient health information in electronic formats (ePHI). This is protected patient information either transmitted by electronic media or maintained on electronic media.

As part of these safeguards, covered entities must institute a contingency plan to be prepared for an emergency, such as a natural disaster or computer virus attack, which could result in a major data loss. This contingency plan must include the following required plans:

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

There are various ways that a healthcare firm can devise a solution that meets these requirements. When choosing a data backup solution, the firm should evaluate the solution's capabilities across six core functionality categories: user authentication, role-based access, data encryption, off-site storage, storage facility security, and reporting.

An online backup solution is one alternative to meet the data contingency plan requirement of HIPAA. In particular, a KeepItSafe® solution can be the perfect fit to meet these core functionality needs with cost-efficiency and low-resource utilization.

Background:
The Health Insurance Portability And Accountability Act[1]

The federal government passed the original Health Insurance Portability and Accountability Act in 1996 as a law designed to:

1. Protect workers from losing their medical insurance coverage if they change or lose their jobs.
2. Reduce the administrative costs of healthcare, specifically by promoting electronic record keeping.
3. Increase the security and portability of patient records.
4. Develop standards for consistency in the healthcare industry

With the exception of small health plans, all covered entities must have had data security standards in place as of April 21, 2005, when the Standards for the Security of Electronic Protected Health Information (the "Security Rule") of HIPAA went into effect for most healthcare providers. Small health plans were exempted until April 21, 2006.

HIPAA was established to protect patient privacy while promoting electronic record keeping. As a healthcare provider it is imperative that you understand the act and its implications for your business.

HIPAA and the Security Rule

The Security Rule requires healthcare providers to put in place certain administrative, physical, and technical safeguards to protect patient health information in electronic formats. This protected patient information is either transmitted by electronic media or maintained on electronic media.

Covered entities that maintain or transmit electronic 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 they create, receive, maintain or transmit.
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information.
3. Protect against reasonably anticipated, impermissible uses, or disclosures.
   Ensure compliance by their workforce.

The Security Rule defines "confidentiality" to mean that electronic protected health information is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the "Privacy Rule" (45 C.F.R. §160) and its prohibition against improper uses and disclosures of protected health information.

The Security Rule also promotes the two additional goals of maintaining the integrity and availability of electronic protected health information. Under the Security Rule, "integrity" means that electronic protected health information is not altered or destroyed in an unauthorized manner. "Availability" means that electronic protected health information is accessible and usable on demand by an authorized person.

The HIPAA Security Rule is designed to support the Privacy Rule by defining security requirements that ensure the integrity, availability, and confidentiality of patient data.

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

In deciding which security measures to use, a covered entity must take into account the following:

1. The size, complexity, and capabilities of the covered entity.
2. The covered entity's technical infrastructure, hardware, and software capabilities.
3. The cost of security measures.
4. The probability and criticality of potential risks to electronic protected health information.

With this information in mind, organizations must adhere to the Security Rule's standards and specifications for safely keeping electronica data.

Covered entities also need to institute a contingency plan to be prepared for an emergency, such as a natural disaster or computer virus attack, which could result in a major data loss. The contingency plan must establish (and implement, as needed) policies and procedures for responding to an emergency or other occurrence (e.g., 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 include the following required plans:

1. Data backup plan. Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
2. Disaster recovery plan. Establish and implement procedures to restore any loss of data.
3. Emergency mode operation plan. Establish and implement procedures to enable continuation of critical business practices 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 their 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 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)).

In addition, covered entities must implement specific technical safeguards (§164.312) to (among other things):

1. Limit access to electronic protected health information only to those persons or software programs that have been granted access rights.
2. Encrypt and decrypt electronic protected health information.
3. Put into place audit controls that record and examine activity in information systems that contain or use electronic protected health information.
4. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

These regulations are in place to ensure that healthcare organizations properly secure their electronic protected health information. Based on these directives, an organization should evaluate its system and implement a secure backup, archiving, and recovery solution to comply with HIPAA standards.

Covered entities must ensure they have a well-defined contingency plan that ensures patient data is still available after a primary data loss. This plan must include backup, recovery, and emergency operating plans. In addition, they must implement technical safeguards to ensure that patient data is properly secured.

Choosing A HIPAA - Compliant Data Backup Solution

Clearly, the contingency plan subpart of the HIPAA Security Rule requires a covered entity to have a solid data-backup plan that meets all of the HIPAA criteria. There are various ways that a healthcare firm can create a solution that meets these requirements.

When choosing a data backup solution, evaluate it across the following criteria:

1. **User authentication.** You should be able to establish private password authentication known only to each user.
2. **Role-based access.** The service authentication-and-access scheme should enable limiting user access only to information they have authority to see.
3. **Data encryption.** All data should be encrypted using the highest encryption standard available before it leaves your location (and, therefore, under the control of your compliant safeguards) and remain encrypted at all times outside of your location. The data should only be unencrypted during a restore after it has been returned to your location. If data needs to be returned from the off-site location to your location via a device (tape, USB drive, DVD, etc.), the data on the device should be delivered in the encrypted state. The solution should also have an option for you to select your own encryption key to ensure that no one without knowledge of that specific key can gain access to the data.

4. **Off-site storage.** It is necessary to have some versions of your backup data stored at a location other than the primary source, in order to provide disaster-recovery capability from similar threats (e.g., floods, hurricanes, electrical outages, etc.).

5. **Secure storage facilities.** The off-site location that stores the remote data versions should have the necessary safeguards to protect against sabotage and natural disasters. A location that has met a SAS70 Type II audit (previous to July 1, 2011), or an SSAE 16 SOC 2 Type II audit (after July 1, 2011) offers assurances that he proper safeguards are in place to meet HIPAA standards.

6. **Solid reporting.** Reports for every backup should be a part of the solution, providing verifiable status data ensuring that the proper resources are monitoring and proactively addressing any potential problems with the solution.

When choosing a data-backup solution, a company should evaluate the solution's capabilities across six core functionality categories: user authentication, role-based access, data encryption, off-site storage, storage facility security, and reporting.

Leveraging Keepitsafe Online Backup For HIPAA Compliance

An online backup service can be the best overall solution to implement a data backup plan, disaster recovery plan, and emergency operation plan that ensures full HIPAA compliance for your company.

However, not all online backup services are equal, and to ensure HIPAA compliance it is imperative that you measure your online backup service against the data backup criteria defined in the previous section. A KeepItSafe solution meets all of these important HIPAA-compliant criteria.

User Authentication

KeepItSafe requires a unique ID and password for creation of backup sets, and that ID and password are required to review the backup sets or restore data from those sets. In addition, an added level of security can be placed on the backup client that is installed on your LAN, requiring an additional password to even access the client.

Role-Based Access

By defining your user IDs and passwords to correlate to your existing HIPAA-compliant administrative guidelines, you can ensure that users are only able to review or restore data that they are authorized to access.

Data Encryption

KeepItSafe individually encrypts each block of data using Advanced Encryption Standard 256-bit encryption technology (AES256). 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. The highest level of AES encryption available for commercial data is 256-bit encryption.

For added security, and to meet the Security Rule's transmission requirements, each encrypted block is transmitted over the Internet via a secure channel using Secure Sockets Layer (SSL) technology – the same Internet transmission technology used by online banking and online credit card applications. With this additional security layer, data is encrypted twice – at all times using the AES encryption, and the encrypted blocks are encrypted once again while they in flight over the Internet, to and from the KeepItSafe data vaults.

Off-Site Storage

With our online backup solution, backup sets that are defined to backup to our vaults give you instant off-site storage of your backup data. You will not need to define a process to get your tapes or disk drives off-site, or pay to have a delivery service pick up and drop off those tapes or disk drives. You can rest easy knowing your most recent backup, and all previous versions that you retain, are safely stored away from your primary data source, preventing them from being subject to any disasters that may affect your primary data location.

Secure Storage Facilities

KeepItSafe may be relied upon to securely back up all ePHI of HIPAA-regulated healthcare business:

1. Our data vaults are housed in redundant Tier-IV data centers.
2. Our designation as a "business associate" (45 C.F.R. 160.103) requires us to sign a business associate agreement (BAA) to signal our acceptance of shared responsibility for HIPAA compliance.

Solid Reporting

KeepItSafe has numerous reporting capabilities ranging from email notifications of backup completion to detailed status and information reports available through our Web interface, the Client Web Operator. In addition, for businesses that use Remote Management and Monitoring (RMM), or Professional Service Automation (PSA) software, we have integrated with most major providers of these systems so status notifications will appear in your RMM and, for resellers or larger IT shops that bill back to the business, billing-data integration into your PSA.

An online backup solution is one alternative to meet the data-contingency-plan requirement of HIPAA. In particular, a KeepItSafe solution can be the perfect fit to meet these core functionality needs with cost efficiency and low resource utilization.

Managing HIPAA Compliance While Managing Your Business

Costs for implementing HIPAA compliance can be significant. Surveys project upgrade costs to vary from $10 thousand for a small private practice to $14 million for a larger organization. The average cost of $3.1 million from surveyed firms is considerably more than the government's projected average estimate of $450 thousand that was done prior to implementation.[2]

Given the overall cost to implement and maintain HIPAA compliance, finding cost-efficient solutions that reduce the total cost of ownership is imperative to successfully managing your healthcare organization.

Online backup – and KeepItSafe in particular – can be one solution that reduces your compliance cost and ensures ongoing peace of mind derived from knowing that your data is fully protected.

KeepItSafe: A Backup Solution that Complies with HIPAA Standards

If you'd like to learn more about how KeepItSafe can help your organization's ePHI comply with strict HIPAA regulations, please contact our data security experts today at **888-965-9988**, or **info@keepitsafe.com.**

Sources

1. All HIPAA requirements are taken from HIPAA Administrative Simplification Regulation Text, Unofficial Version, as amended through February 16, 2006. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf>

2. Arora, Richa and Pimentel, Mark. Cost of Privacy: A HIPAA perspective, December 9, 2005. <http://lorrie.cranor.org/courses/fa05/mpimenterichaa.pdf>