ShareSync and HIPAA Compliance

Contents

For many organizations, the decision to move to the cloud is about economics: the cloud provides greater value than an on-premises deployment.

But for healthcare providers or organizations that work with Protected Health Information (PHI), there's a consideration beyond economics: the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Here's how this impacts you: you need to make sure that your cloud service providers can support HIPAA compliance—because if they're not able to do that, you won't be able to achieve or demonstrate HIPAA compliance.

> **ShareSync services are designed to meet the privacy and security requirements for Protected Health Information. Our privacy and security policies, procedures, technologies and services are audited annually by a third party, and we will execute a HIPAA Business Associate Agreement with Covered Entities.**

File sharing and syncing

Of course, your handling and use of protected patient health information is not just a matter of email content and attachments.

We live in an age of digital health records and specialized, collaborative health care and administration. To deliver the best care efficiently and economically, multiple parties, both within and outside your organization, need access to your patients' electronic health information. But that imposes a complex set of requirements on your IT systems, including:

- **Security.** HIPAA imposes an absolute responsibility for maintaining the privacy and confidentiality of patients' health records, both at rest and in transit. This means you have to provide and control multiple levels of access to that information for the many people who collaborate on patient care and related services—that is, your many diverse partners as well as your staff. And you have to be able to monitor and audit all health information file access, use and change, both inside and outside your organization.

- **Integrity**. To secure electronic protected health information (ePHI) from improper change or destruction, you must control not only who has access to what information but also who can change a file and when.

- **Mobility.** Mobility has come to medicine. You may already deploy authorized mobile devices, such as Wi-Fi-connected cart-based PCs in hospital wards and personal tablets for clinicians. Chances are, more and more staff want and need to connect with your network-based applications and files from mobile devices, whether issued by you or purchased by them (a trend known as BYOD, or bring-your-own-device). Mobility adds another significant layer of complexity to the task of providing secure, HIPAA-compliant file access.

ShareSync HIPAA Capabilities

Mobility and HIPAA Compliance

ShareSync offers doctors, medical researchers and medical administrators a quick way to securely back up and share files that contain PHI. ShareSync supports HIPAA compliance and signs HIPAA Business Associate Agreements with its customers.

File Sharing Compliance - Improve Healthcare Coordination

ShareSync helps teams inside and outside of healthcare organizations work together by streamlining the secure sharing of administrative and patient information.

Medical departments rely on extensive file sharing of test results, patient data and lab practices. Traditional methods of sharing files over email, FTP and USB drives have security flaws, and often run the risk of violating HIPAA, HITECH and FDA regulations. ShareSync allows you to securely share sensitive files behind the firewall, without a VPN.

ShareSync also offers organizations a secure method to share specific folders and files of any size. ShareSync enables users to create shared, permission-based folders, for collaboration across internal and external teams. Individuals can use ShareSync to ensure specific files are sent securely by creating password protected web links.

Collaborate on Research

ShareSync allows for secure collaboration across multiple departments inside healthcare organizations and with outside contracted research partners. Collaborate on research, journals, grants and teaching materials. ShareSync has Microsoft Office plugins that help distributed teams and departments work together on the same set of files, as if they're in the same office.

Increase Productivity

Keep materials available in real-time to remote employees out in the field. ShareSync gives agents access to the latest files, through virtually any device.

ShareSync includes features like automatic file versioning that ensures when a change is made to a file stored on ShareSync, a newer version is automatically created and added to the folder containing the earlier version. File versions are time-stamped and include the name of the user who made changes to the file. Users can even subscribe to be notified when changes are made by other collaborators.

Security Control, Visibility and Auditing

Saving critical company data such as lab results and drug approval processes on personal laptops or mobile devices can lead to serious security issues. ShareSync addresses the security needs of medical companies by providing complete control over folder access and real-time visibility on all user activity.

Administrators can deactivate user accounts as needed (e.g., when an employee leaves the company) and easily assign and revoke permissions on any folder. ShareSync also provides administrators with a rich set of controls such as audit reporting, administrative access to all ShareSync content, retention policy for past file versions and delete files, external sharing policies, and remote wiping of lost or compromised devices

Data Security & Protection

Customer Data on ShareSync

- 256-bit encryption for at-rest and in-transit data.
- Unique encryption key for each account (much better than sharing keys between customers)
- 99.999% uptime SLA.
- SSAE 16 SOC2 Type II Reports.
- Reporting and audit trail of account activities on both users and content.
- Administrators can remotely wipe data from any registered device.
- Ability to grant specific access permissions to each collaborator.
- Locking features to prevent overwrites, conflicts or deletions.
- Secure file links sent inside and outside your organization.

Datacenter

- Global Intrusion Prevention System protects cloud services.
- Datacenter-level backup and file replication protects against loss or corruption of information.
- Datacenters guarded by video monitoring, motion detection and access control technology as well as 24/7 security personnel.

ePHI security and integrity

- Security systems that guard against unauthorized access to ePHI during electronic transmission, whether in email and attachments or during the file-sharing process.
- Both electronic and physical security to protect ePHI wherever it is stored. Technology and policies to secure ePHI from improper alteration or destruction.

Four Important HIPAA Compliance Concerns

If you're concerned about HIPAA compliance, don't be.

1. We will sign a Business Associate Agreement
2. We undergo SOC 2 Type II audits
3. We provide white-glove onboarding
4. We support you 24/7

Remember, ShareSync covers your HIPAA needs.

For more information about ShareSync's HIPAA features—or to request a live product demonstration—feel free to contact us.