Safeguard protected health information with ShareFile

This enterprise file sync and sharing solution supports HIPAA compliance, boosts security and mobilizes data access

ShareFile helps healthcare providers securely exchange large files with medical groups, health systems, payors, patients and other third parties without the complexity of using FTP sites or faxes or the delays associated with courier or postal services.

CİTRİX®

Safeguarding protected health information (PHI) is a major priority for healthcare organizations. The 1996 Health Insurance Portability and Accountability Act (HIPAA) provides a framework for the legal protection of patient-specific healthcare data today. Any firm operating in the healthcare industry must adhere to HIPAA's stringent security requirements that protect patient data shared by physical or virtual means. An additional HIPAA rule, the Omnibus Final Rule added in 2013, states businesses that interact with and transmit PHI are subject to enhanced rules and penalties for noncompliance with the law. Organizations are turning to secure, healthcare-specific, cloud-based IT solutions that address these rules and further reduce the risk associated with a breach of PHI. Many healthcare IT teams are deploying enterprise-grade file sync and sharing tools to address security of patient records.

Healthcare industry challenges
- Comply with HIPAA requirements

- Leverage current IT infrastructure investments – connect to existing network shares, SharePoint or ECM systems

- Enhance patient care quality with easy yet secure access to patient healthcare information

- Improve employee productivity via instant access to corporate data and personalized desktops from any device

ShareFile is an enterprise-grade, HIPAA-compliant file-sharing solution. ShareFile gives healthcare organizations a choice of where data is stored – on premises, in a dedicated healthcare cloud or a combination — to meet individual needs. IT can provide instant mobile access to data, including information on existing network drives and SharePoint sites. Caregivers can access, sync and securely share files within their delivery network and with ancillary providers. Clinical staff can send discharge instructions and wellness resources to patients and track download statistics. Offline access and integration with email simplify secure file sharing.

ShareFile addresses key business requirements that healthcare organizations face today:

- Safeguard PHI
- Send and receive confidential files with encryption to maintain HIPAA compliance
- Prevent information leaks and security breaches
- Increase mobile productivity and collaboration
- Provide IT with controls and tools such as robust reporting, file tracking and usage auditing

ShareFile for healthcare empowers mobility and provides organizations with the power to share and protect PHI with tools that are easy for everyone to use.

Safeguarding PHI
ShareFile allows IT to determine how sensitive data is stored, accessed and shared. Advanced security features including remote wipe, device lock, passcode protection, white/black listings and data expiration policies ensure complete control over enterprise data, regardless of where it is located. Robust reporting and

ShareFile delivers business results

- Easily and securely send and receive confidential healthcare files with encryption

- Address HIPAA rules for confidential PHI with a private enclave dedicated to healthcare

- Boost security and gain IT control of how PHI is stored, accessed and shared

- Enhance collaboration in real time with features that facilitate data exchange

auditing features enable IT to track and log user activity in real time and create custom reports to meet corporate data policies and compliance requirements. Seamless integration with enterprise directory services simplifies authentication and user provisioning.

ShareFile provides additional safeguards unique to healthcare to support customer compliance obligations under HIPAA. Many of these controls are not configured by default and require configuration setup during ShareFile deployment.

- **Audit controls** - Customers can use the tools provided within ShareFile to review account activity, such as account usage and access to files and folders.
- **Unique users and authentication** - ShareFile lets customers create individual user accounts based on unique email addresses. For easier access and enhanced authentication security, customers also can integrate with a SAML 2.0-compatible identity management solution to enable single sign-on.
- **Emergency account access** - Account administrators on the customer side are the only people with total authorized access to their ShareFile accounts. Customers are responsible for assigning emergency access to PHI stored in ShareFile in the event the account administrator is unavailable.
- **Session timeout** - ShareFile gives customers the technical ability to automatically log out a user after a period of inactivity. Customers can define the length of this period of inactivity, and they are responsible for enforcing an automatic logout period consistent with their internal policies. ShareFile also provides a button that lets users log out of a session at will.
- **Encryption** - ShareFile handles the encryption and decryption of all files, including those containing PHI. Users can, at their discretion, also encrypt files prior to uploading. If a user

chooses to do this, ShareFile will still automatically encrypt files a second time. Files are transferred through ShareFile over a secure SSL/TLS connection and are stored at rest with AES 256-bit encryption.
- **Integrity controls** - To help ensure that PHI has not been altered or destroyed in transit or at rest, ShareFile uses industry-standard hashing algorithms to verify file integrity during upload and download.
- **Passwords** - ShareFile gives customers the technical ability to set a unique password for each user account. ShareFile password policy parameters include password expiration, history and minimum length. Customers can configure password complexity controls according to their own internal policies. ShareFile can also integrate with identity management solutions that are compatible with SAML 2.0.
- **Account lockout** - By default, ShareFile locks out a user for five minutes following five failed login attempts. ShareFile configures these settings as account preferences to satisfy customer requirements. Customer-definable lockout settings are available upon request.

Send and receive confidential files to maintain HIPAA compliance

With ShareFile, all file types can be securely shared digitally with anyone, either internal or external to the organization. Very large files can be shared. Users can preview all Microsoft office files and PDFs within their web browsers. Built-in mobile editors can be leveraged to permit free-form signatures on documents.

The Send a File feature enables companies to collect sensitive patient documents from third parties without giving them access to their central system. Some companies have found this useful for collecting medical test reports from other facilities to accelerate care.

The ShareFile Cloud for Healthcare is a dedicated, secure storage space within a private cloud where customers can have PHI processed and stored. This private cloud, which hosts multiple customers, is reserved for those in industries that process or store PHI, such as healthcare, insurance and financial services companies. The ShareFile Cloud for Healthcare is technically compliant with the HIPAA Omnibus Final Rule.

Customers wishing to use the ShareFile Cloud for Healthcare must sign and return a Business Associate Agreement (BAA) to Citrix before ShareFile can provision their account. ShareFile maintains a BAA for each covered entity, such as a hospital, doctor's office or health insurance provider, and a separate BAA for business associates such as accounting or consulting firms that work with these covered entities. Customers designated as a covered entity

under HIPAA must sign the Covered Entity BAA before using ShareFile to process and store PHI. Similarly, customers designated as business associates under HIPAA must sign a Business Associate BAA. There is no additional cost to join the ShareFile Cloud for Healthcare.

For information on how the ShareFile Cloud for Healthcare supports your efforts to comply with the HIPAA Omnibus Final Rule, read the ShareFile Cloud for Healthcare Whitepaper.

Easily and securely exchange files

ShareFile offers several built-in features that permit easy and secure exchange of confidential patient files inside the organization and with external healthcare providers, medical groups, health systems, payors, patients and other third parties:

ShareFile

Send from ShareFile ›
Send a File ›
Request a File ›

Email
Password

Sign In

Email integration

With the ShareFile Plug-in for Microsoft Outlook®, users can securely send files to patients, insurance companies or other parties with the proper PHI guidelines, instead of faxing them. File tracking and alerts notify users when recipients download documents.

Patient portal

Easily share confidential records, information and forms with patients using the ShareFile patient portal. No software downloads are required, so patients can quickly access this secure portal.

Prevent information leaks and security breaches

Organizations have the flexibility to choose where data is stored – on premises, in the cloud or a combination — to meet their specific requirements for data sovereignty, compliance, performance and costs. For organizations that require increased data protection, ShareFile offers customers the ability to encrypt data with their own encryption keys. By defining where data is stored, IT can build the most cost-effective and customized solution for the organization. ShareFile with StorageZones also allows IT to take advantage of the economic benefits and effortless management of a cloud-based service.

Files are transferred through ShareFile over a secure SSL/TLS connection and are stored at rest with AES 256-bit encryption. Through the Passcode Lock feature, IT can leverage the mobile device's encryption capabilities and enforce encryption for all ShareFile data on the device. The data centers that host the ShareFile web application and databases are SSAE 16 accredited and the data centers that host the file storage application are SSAE 16 and ISO 27001 accredited. Citrix implements and maintains commercially reasonable and appropriate physical, technical and organizational controls to protect customer data. ShareFile is PCI-DSS compliant and will enter into a HIPAA BAA.

Enforce data security policies for sensitive and confidential data by integrating ShareFile with existing DLP (data loss prevention) systems to restrict document sharing based on the file's DLP classification. ShareFile integrates with popular DLP systems (Symantec Data Loss Prevention, McAfee DLP Prevent, Websense TRITON® AP-DATA, RSA Data Loss Prevention and others) for Customer-managed StorageZone deployments only. Enterprises, especially those in highly-regulated industries, need to be able to control file sharing based on the content inside the files themselves. Connecting ShareFile with customer's existing DLP system allows ShareFile to classify files based on their content and enforce sharing restrictions per company policies.

Increase mobile productivity and collaboration

ShareFile provides users with a true enterprise-class data services across all corporate and personal mobile devices, while giving IT all the control it needs. Users can access, sync and securely share files from any device with people both inside and outside the organization for easy collaboration and enhanced productivity. ShareFile seamlessly integrates with workflow tools such as Microsoft Outlook and provides a rich user experience on any device to enhance productivity. Offline access keeps productivity up even when on the go.

Assigned users can securely access files from any device (desktops and mobile devices) and from any location. ShareFile offers a full suite of intuitive mobile apps that make data accessible anywhere, such as at the office, at the hospital or during a patient visit.

IT control and reporting, file tracking and usage auditing

For IT, ShareFile provides comprehensive capabilities to track, log and report on user file access, sync and sharing activity, including the date, type, place and network address of each user event. IT can enable tracking through workflow tools such as the Plug-in for Microsoft Outlook. Multiple versions of files can be stored to create full audit trails of editing activity. IT can also track remote wipe activity on a device from the time the wipe is initiated through its execution, and will receive a notification indicating whether the wipe has succeeded. IT can create custom reports on account usage and access.

IT can control specific user rights to ShareFile. Users can be granted download-only access or full upload/edit/delete rights depending on their location, role, device and other criteria. Some organizations set up ShareFile logins with defined password complexity for each user account, restrict the number of downloads available to a given user, restrict upload and download permissions for users and define length of time for folders and links to expire. IT can also restrict access based on network location and can blacklist/whitelist email domains to control data sharing. IT can also limit access to the Sync feature for specific users, such as those with managed or corporate devices.

ShareFile is available in multiple languages: English, French, German, Spanish, Japanese, Korean, Simplified Chinese, Russian, Dutch and Portuguese.

Conclusion

ShareFile is an enterprise file sync and sharing solution that supports HIPAA compliance, boosts security and mobilizes data access. ShareFile helps healthcare organizations, which operate in complex legal and security-intensive environments, safeguard PHI. Healthcare workers can quickly and efficiently send and receive confidential files while maintaining HIPAA compliance ShareFile also addresses top concerns of healthcare IT to prevent information leaks and security breaches. Healthcare IT managers now have the tools they require with an enterprise-ready and secure solution that helps control how data is accessed, stored and shared.

Learn how the ShareFile Cloud for Healthcare helps healthcare providers meet compliance requirements and reduce inefficiencies.

Citrix, a trusted partner to healthcare providers

Citrix is the trusted solution partner for 90 percent of the world's largest healthcare providers, all of the US News & World Report top hospitals for 2014 and all the top health information technology vendors. Millions of clinicians and staff rely on healthcare IT solutions from Citrix to deliver seamless, secure, instant access to patient information as they roam across facilities, devices and networks.

Citrix offers additional solutions that enable healthcare IT leaders to centralize and streamline IT operations and infrastructure to reduce overhead and gain efficiencies that will transform their business:

- **Clinical mobile workspace** - The Citrix mobile workspace delivers an always-on, always-connected, personalized working environment by securely uniting clinical and non-clinical Windows, web and mobile applications, desktops, files and services into a single workspace tailored to a person's role or medical specialty.
- **Instant, secure access to clinical and business applications** – With XenApp, IT can instantly deliver clinical and business software – like EMRs, imaging viewers and revenue cycle management solutions – to people working across distributed facilities. Clinicians and staff gain real-time access to applications from any device, including zero and thin clients, tablets and home PCs.
- **Clinical-grade desktops for roaming caregivers** – With XenDesktop, IT can deliver a tailored desktop for unique medical specialties or functions, from personalized desktops for doctors, to standardized,

locked-down environments for hospital staff, to client-side virtual desktops for secure offline use by executives. Virtual desktops make it easy for clinicians to roam from one device and location to another without interrupting their workflow.

- **Securely adopt mobile devices and new mHealth apps** – With XenMobile, IT can embrace mobile devices and apps while maintaining the control needed to track devices, secure access to sensitive data and ensure compliance with HIPAA, PCI-DSS and corporate policies. ShareFile integrates with XenMobile for mobile content management to allow employees to access, sync and securely share files from any device with people both inside and outside the organization. ShareFile is included with XenMobile Enterprise licenses and is also available as a standalone enterprise file sync and sharing solution.

- **Combining ShareFile and XenMobile delivers additional security features** - Healthcare organizations can restrict access to data based on user location, sometimes referred as geo-fencing. Data files are stored electronically in ShareFile. An IT administrator can assign specific requirements to control who can view these confidential files and from which locations. For example, IT might specify that patient data files can only be viewed while the user is in the hospital; after leaving the building, the files can no longer be viewed.

"ShareFile gives me the ability to put tools in the hands of novice computer users and allow them to easily send/receive large files and secure files. In the hospital environment, it makes the compliance officer (me) feel much more at ease."

Steve Taylor, compliance officer for Anderson Regional Medical Center

"ShareFile offers simplicity for our employees and clients with the "request a file" feature. We chose Citrix because it's an industry standard."

Nick Munger, director of information technology for POMCO Group

Corporate Headquarters Fort Lauderdale, FL, USA	**India Development Center** Bangalore, India	**Latin America Headquarters** Coral Gables, FL, USA
Silicon Valley Headquarters Santa Clara, CA, USA	**Online Division Headquarters** Santa Barbara, CA, USA	**UK Development Center** Chalfont, United Kingdom
EMEA Headquarters Schaffhausen, Switzerland	**Pacific Headquarters** Hong Kong, China	

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

CiTRIX ®