White Paper

Filr

Taming the Mobile File Sharing Beast—Healthcare

The healthcare industry is going mobile in droves as providers recognize the gains in organizational efficiency–and patient outcomes–that come when data is available anytime, anywhere. With the continual innovations and advantages mobility offers, it's no wonder that 85 percent of hospitals allow clinicians to use their personal mobile devices at work. Greater mobility leads to greater productivity, after all. Unfortunately, not only do most mobile file access and sharing solutions lack the security and compliance healthcare organizations need, but they stifle user productivity and increase IT management efforts, as well. The good news is that striking the right balance between enabling mobile productivity and safeguarding protected health information (PHI) just became a lot easier.

MICRO FOCUS

Assessing the Different Classes of Mobile File Access Offerings

The healthcare industry is going mobile in droves as providers realize the gains in organizational efficiency—and patient outcomes—that come when data is accessible anytime, anywhere.

Mobile apps not only make it easy for doctors to check patients' records or examine their x-rays, but medical apps can give a smartphone or tablet the ability to diagnose abnormal heart rhythms, take ultrasounds, execute treatment orders in real-time, and more. With the continual innovations and advantages mobility offers, it's no wonder that 85 percent of hospitals allow clinicians to use their personal mobile devices at work. Greater mobility leads to greater productivity, after all..

Similarly, according to PwC, 75 percent of hospitals allow employees to access electronic health records (EHRs) on those personal devices. Unfortunately, only 46 percent of those hospitals have a security strategy governing the use of mobile devices. This lack of mobile security can have serious HIPAA implications that can lead to breaches of protected health information (PHI), significant fines and even lawsuits. In spite of these risks, however, mobile file access and sharing will continue to increase as more facets of the healthcare industry view mobility as a workplace necessity.

You might already be looking at mobile file access and sharing solutions that appear to be healthcare-friendly. If so, you're on the right track. But be aware that among the different classes of solutions available, many lack security and compliance-readiness, stifle user productivity and create additional work for IT teams that are already stretched far too thinly.

So, how do you mitigate the risks associated with mobile file access and sharing? Provide your users with a solution that's simple to use—and that doesn't disrupt the security and compliance infrastructure you've already created for your file system. Cloud solutions might seem like a good fit at first, but the risks involved in using the cloud solutions available today can quickly wear you down. The good news is that striking the right balance between keeping mobile users productive and keeping PHI secure is not as difficult as you might think.

Cloud Services Fall Short of Needed Governance and Compliance

An independent study indicates that of the healthcare organizations that use cloud services, 47 percent of them have no confidence their information in the cloud is secure, and another 23 percent are only somewhat confident (*Ponemon Third Annual Benchmark Study on Patient Privacy & Data Security*, December 2012). Additionally, under the new HIPAA omnibus rule, healthcare organizations that use cloud services for sharing or storing files not only have to be HIPAA-compliant themselves, they also have to secure a HIPAA Business Associate Agreement that holds their cloud provider equally liable.

In Europe, using the cloud for mobile file access and sharing might not even be a viable option for healthcare organizations. The European Union Data Protection Directive imposes stringent rules that often prevent data from being stored in public clouds, and in some cases, even private clouds. Whether in the U.S., Europe or elsewhere, compliance with such rules and regulations is only the beginning of the problems associated with turning to the cloud for enterprise mobile file access and sharing.

Consumer-Grade Cloud Services

Whether it's compliance with HIPAA, EU Data Protection Directives, or other data protection regulations, you can't afford to let users drive the mobile file access agenda with consumer-grade cloud services like Dropbox, Google Drive, or SkyDrive. These services make it easy for users to sign up and start using the service right away. But the primary focus of these services is usability for the masses, not regulatory compliance or PHI security.

Mobile apps for consumer-grade cloud services are typically not conducive to regulatory compliance. Additionally, these consumer-oriented services lack the authentication controls and enterprise-class security you've already established and depend on within your own infrastructure.

You have little control, if any, over what files users can store in— and share from—these services. And what happens to the files in an individual's cloud storage account if the user leaves your organization or gets laid off? Because they involve moving your data, consumer-grade cloud storage services leave you out of the governance loop and prevent you from knowing where your files actually go.

Enterprise-Targeted Cloud Services

In an attempt to fill the compliance and security void left by consumer-oriented cloud services, other cloud solutions have surfaced, claiming to meet the needs of professional and healthcare organizations. These services tout enterprise-class security and control, giving IT administrators the ability to manage access rights and authentication policies. This offer of enterprise-grade security and IT control has its appeal, especially when coupled with the promise that it will free you from the burden of hosting and managing that storage infrastructure. Perhaps it seems like the perfect solution to securely address your mobile users' file access and sharing needs. Not so fast. So-called enterprise-grade cloud storage services have four main failings.

Questionable Compliance

As previously mentioned, new HIPAA omnibus rules require your cloud service provider to be HIPAA-compliant, and EU Data Protection Directives may prohibit you from storing your healthcare data in the cloud to begin with. In the case of HIPAA, even if your cloud provider signs a Business Associate Agreement, what guarantee do they really provide you that they'll stay compliant and adequately protect your PHI? The terms of many cloud providers' service-level agreements (SLAs) specifically limit their liability, even if they experience a breach or fail to meet compliance standards. With the threat of fines and lawsuits looming large, how much control do you really have in ensuring your cloud service provider remains compliant?

Duplication of Management Effort

Enterprise-targeted cloud services result in duplication of management effort. You've likely spent several years establishing and fine-tuning the security controls and access privileges for your healthcare data. These solutions invite you to tackle that arduous process all over again, but this time using their security tools instead of the ones you already know and trust. You also earn the ongoing opportunity to manage security for your existing in-house data infrastructure and this new hosted infrastructure separately.

Empty Data Repositories

One of the most important and often overlooked failings of enterprise cloud services for mobile users is the need to repopulate data from your established infrastructure to the cloud. You need to take a realistic look at how many weeks or months of effort it will take to move all those files to your new cloud storage. Do you move all of them? Some of them? Is it a complete move or just a copy, leaving you with duplicate data? How will you know which files your users really need or want in the cloud?

The reality is that in many organizations. IT leaves it to the users to decide what to migrate. For some businesses that might make sense, but for healthcare organizations the issue is significantly more complex. Users may inadvertently move sensitive information to the cloud. Worse yet, they may become overwhelmed by the options and procrastinate migrating any data at all, leading to empty cloud repositories. As a result, you are left with no guarantee that your mobile users will ever be able to actually access and share data from this new service you've invested in.

File Duplication and Version Control

When you're copying files from your on-premise repository to a hosted cloud service, you're likely to end up with file duplication and version control issues. Users might not always remember or know which files have been moved to the cloud. One day they work on a version in the cloud, and then a week or two later they make changes to the version stored on the enterprise file server. This becomes even more likely—and troublesome—with shared files, where different users work on multiple versions stored in various repositories. Some so-called enterprise cloud services do include auditing tools to address version control problems, but they're only effective if you do a complete migration of your files.

Hybrid/On-Premises Solutions

To address some of the deficiencies in enterprise-targeted cloud services, a few vendors have started offering a hybrid service for mobile file access and sharing. While their focus is to move most of your files to the cloud, these hybrid services allow organizations to store some of their files in the provider's cloud service and others in the organization's on-premises data centers.

By empowering organizations to leverage their own data center infrastructure for mobile file access and sharing, these hybrid solutions definitely take a step in the right direction. On-premises storage, after all, not only gives you greater control and oversight over your data, it helps you meet regulatory and compliance requirements, as well. Unfortunately, with their objective to move most of your data to the cloud, these hybrid solutions share many failings with enterprise-targeted cloud services.

Allocation of New and Separate Storage

Even though hybrid services allow organizations to leverage their on-premises data center and equipment, the organizations still have to allocate new and separate storage for housing the mobile data. Obviously, the movement of data from an old on-premises data store to a new

on-premises data store won't be as monumental as moving all those terabytes across the Internet. But you'll still encounter questions related to what files get moved, who moves them, and how to deal with potential duplication of data.

Lack of Real Integration with Existing File System
The bigger problem is that even if your mobile data stays on-premises, your mobile file shares are not really integrated with your other existing file shares. Some hybrid solutions offer a level of integration with Active Directory, but you're still dealing with a new file system. Once again, you face the significant effort of re-creating and reconfiguring all of your established file access controls for the data moved into that new system.

Rather than managing a single file system infrastructure, you now have to manage two separate infrastructures. And, as with enterprise cloud services, managing your hybrid solution will require you to use a separate set of management utilities.

Investment in Added Data Management Processes
These hybrid services add complexity to your environment. Since they're not really leveraging your existing file service, they're also not leveraging all the existing processes you have in place for managing your data. For example, how will you back up these new mobile repositories? How much effort will it require to rework your existing backup services to encompass the new data stores? How many man hours will it take to integrate your existing healthcare management systems with the hybrid environment? What other workflows and services will you have to reconfigure to accommodate a hybrid mobile file access and sharing solution?

On-Premises, File System-Integrated Solutions

In the attempt to create greater mobile productivity, all the services and solutions described thus far put healthcare organizations at greater risk, create more management complexity, fail to meet users' needs or create a combination of all these problems. The best way to comply with healthcare data protection regulations and securely deliver the mobile file access and sharing your users need is to rely on a solution that uses the files and file systems you already have in place.

Leverage Existing Files, File Systems, Processes and Controls
Whether in the cloud or on-premises, users don't need yet another set of files or another repository for accessing data on the move. They just need to be able to access and share their existing files from where they're already stored. And IT doesn't need or want another file system to manage, let alone have to use completely new tools to manage it. They just need to mobilize their existing file systems in a way that utilizes the security infrastructure, file access controls and data management processes in which they've already invested.

Compliance, Collaborative Sharing and More
Even with an on-premises, file system-integrated offering, you need to verify that it delivers all the functionality your users need and the regulatory compliance you require. In addition to intuitive mobile file access, does it leverage your security infrastructure and data governance policies? Do the controls for file sharing and mobile downloads provide the granularity needed to comply with healthcare industry regulations and data protection directives?

Does the solution enable mobile users to easily and quickly search across all their authorized file shares to find the content they need? Does it allow native commenting and collaboration on shared files, or do users still have to resort to email or other forms of communication to provide context for the files they've shared?

Only Micro Focus® Filr delivers on all those counts, providing the complete, on-premises file system integration healthcare organizations need and the mobile file access and collaborative sharing their users demand.

Mobile File Access and Sharing Healthcare Can Embrace

Whether in the cloud or on-premises, other mobile file access vendors make plenty of promises, but they can't stack up to the balanced approach of Filr, which delivers all of the following benefits:

- Use of and adherence to an organization's established data protection policies, user access controls and quotas, so the same group and user access rights that govern your organization's home and network folders also govern mobile access
- Seamless integration with users' existing folders, including home directories and network shares, giving users secure mobile access to all of their enterprise content on day one
- Utilization of users' real credentials for file access, ensuring authorized access and audit trail support
- Managed connections between existing file servers and your endpoints, including Windows and Mac devices, iOS, Android and BlackBerry mobile devices, as well as standard web browsers
- Non-intrusive and easy-to-deploy virtual appliance with no need to deploy server agents, extend your schema, or invest in new data center hardware
- Support for multiple identity stores, including Microsoft Active Directory and Micro Focus eDirectory™
- Native file system integration with Microsoft Windows Server and Micro Focus Open Enterprise Server (CIFS and NCP)
- No file migration or duplication, since files remain on existing enterprise file servers

- Easy-to-use, “follow me” file synchronization
- Granular control over mobile file downloads
- Granular control over file sharing, including the ability to determine which files and folders users can share either internally or externally

Keep Mobile Users Happy and IT in Control

Unlike other mobile file access and collaborative file sharing solutions, Filr caters to both your PHI governance needs and the desires of your mobile users. It requires less administration, delivers better security and results in happier users. It lets you leverage your established security and data protection infrastructure, while giving users easy, anywhere, any device file access. Your users get the mobility they want, while you stay in control of managing your confidential records, ensuring regulatory compliance, and earning the public trust.

To learn more about how your users can enjoy the productivity gains and time savings of mobile file access and collaborative sharing without compromising security and compliance, visit **www.novell.com/filr** or contact us at 888-321-4272.

About Micro Focus

Since 1976, Micro Focus has helped more than 20,000 customers unlock the value of their business logic by creating enabling solutions that bridge the gap from well-established technologies to modern functionality. The two portfolios work to a single, clear vision—to deliver innovative products supported by exceptional customer service. **www.microfocus.com**

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Provo, Utah
801 861 4272
888 321 4272

Additional contact information and office locations:
www.novell.com