



# Meeting Healthcare Demands for Mobile File Access and Sharing

The healthcare industry is going mobile in droves as providers recognize the increased efficiency and higher standard of care professionals can deliver using smartphones and tablets. 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. But how do you strike the right balance between enabling your mobile users and keeping protected health information (PHI) secure?

## Filr at a Glance:

### ■ Ease of Use:

Filr requires less administration and delivers better security, resulting in higher productivity for end users and IT alike.

### ■ Easy Access:

Filr lets you leverage your established security and data protection measures, while giving users easy, anywhere, any-device file access.

### ■ Stay in Control:

Mobile users get what they want, while you stay in control of your organization's confidential records and information.

## Assessing Healthcare Options for Mobile File Access and Sharing

The demand from healthcare professionals for mobile file access and sharing continues to rise as mobility becomes a workforce necessity. How do you mitigate the risks associated with mobile file access and sharing? You provide 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.

## Cloud Services Fall Short of Needed Governance and Compliance

Independent studies indicate that of the healthcare organizations that use cloud services, 47 percent 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 with their cloud service provider that holds the provider just as 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 organizations from storing information 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 mobile file access and sharing.

## Consumer-Grade Cloud Services

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. Further, they involve moving your data, which leaves you out of the governance loop and prevents you from knowing where your files actually go.

**The best way to stay HIPAA-compliant and 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: OpenText Filr.**

Connect with Us



### Enterprise-Targeted Cloud Services

Enterprise-targeted cloud services tout enterprise-class security and control, but they have significant, inherent failings. First and foremost, cloud data repositories are only useful after someone has taken the time to populate them with files; if this work isn't done, you've invested in nothing more than an empty container. These services also leave you at the provider's mercy in terms of compliance and adequate protection of your patients' PHI.

### Hybrid/On-Premises Solutions

Even though hybrid services allow you to keep some of your files in your organization's on-premises data centers, the providers' focus is to move mobile files to the cloud. As a result, hybrid services suffer from many of the same failings as enterprise-targeted cloud services. Additionally, these services double your management effort, essentially requiring you to manage two separate infrastructures.

### The Answer: On-Premises, File-System-Integrated Solutions

The best way to stay HIPAA-compliant 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. You need a solution that can mobilize your existing on-premises file system in a way that leverages the security infrastructure, file access controls and data management processes in which you have already invested.

### Mobile File Access and Sharing Healthcare Can Embrace

OpenText™ Filr gives your users easy, anywhere, any-device access to your organization's files, while keeping the process completely under your organization's control. It delivers the mobile file access and collaborative file sharing users want, but through an enterprise-ready design that leverages your existing infrastructure and established controls. It eliminates the need to manage third-party services or create and manage hybrid file stores by allowing you to use your existing file servers, existing files and existing file system rights.

Filr supports iOS, Android and BlackBerry mobile devices, as well as standard web browsers. It works in Microsoft Active Directory environments and integrates natively with Microsoft Windows Server and Windows-compatible storage appliances.

To learn more about how your healthcare professionals can enjoy the productivity gains and time savings of mobile file access and collaborative sharing without compromising the security of your PHI, visit [www.microfocus.com/en-us/portfolio/file-sync-and-share](http://www.microfocus.com/en-us/portfolio/file-sync-and-share).

Learn more at [www.opentext.com](http://www.opentext.com)