CITRIX®

White Paper

Six steps to enabling the mobile clinician for the future

Empower mobility, ensure security, and position your healthcare IT environment for the future of patient care

Healthcare IT is a driving force in bringing about better patient care, and mobility is a key component. Mobility in the healthcare world is unique: clinicians roam from one shared workstation to another, use their tablets on rounds, check data on personal smartphones, and work on home computers. They need to access clinical systems and vital patient data on any system at any time. But the benefits of mobility bring hefty requirements for IT, especially as healthcare entities embrace the journey to cloud computing.

Clinicians demand easy access to clinical apps and patient data. They want their user experiences to be consistent and familiar on a variety of devices. You have to ensure constant data protection, privacy of protected health information (PHI), and compliance with HIPAA, MACRA and other regulations that govern the use of information and the delivery quality of patient care.

Your IT environment is becoming more complex by the day, so you're probably looking for ways to reduce costs and improve efficiency. The good news is that, if you implement mobility right, you can deliver on-demand data, applications, and desktops to any device over any network, and maintain security, compliance, and control. This implementation can lead to significant time savings for clinicians and can actually reduce costs while making life easier for IT. Here are six steps that provide a rational path for you to plan, define, and roll out a mobility initiative in your healthcare organization that will help you reap benefits today and in the future.

Step 1: Embrace industry best practices

Mobility management in healthcare used to mean simply controlling devices; now it's about controlling the apps and data clinicians need to access as they roam throughout the hospital. Defining policies around patient data and app management requires early engagement and buy-in from a variety of stakeholders including Security, HR, Legal, and key personnel such as the CMO and CNO. Policies need to address clinician demands without impacting an organization's security posture. Key aspects include eligibility, allowed devices, services and app availability, device and user support, and legal terms of use.

Today's IT environments also include cloud technologies and complementary third-party solutions. There's a lot to manage and integrate. It's important to partner with vendors that can help you at any stage of the cloud journey — and with those who have a large ecosystem of partners with whom they work continually.

Step 2: Define your technology strategy

In healthcare, when defining your technology strategy, it's crucial that your software vendor has a proven track record in enabling clinician mobility. That vendor should be able to partner with you regardless of your stage in the cloud journey. The technology offered should not impact IT control and security. Effective clinician mobility enablement requires many capabilities: desktop and application virtualization, file sharing, cloud computing and cloud networking, mobility management, and more.

Best practices indicate you should look to solutions that provide persistent data and app availability, ensure secure user-friendly mobility, and — with a minimum effort on your part — deliver a consistent, familiar and reliable user experience on any device. For a number of years, Citrix has been in the vanguard of healthcare mobility, developing solutions that incorporate the collective knowledge of thousands of implementations. Steps 3-6 discuss key requirements.

Step 3: Select technologies to provide 24/7/365 app and data availability

Centralized management and delivery of clinical applications, such as electronic health records (EHRs), medical imaging applications and legacy applications, can be addressed through app and desktop virtualization and/or cloud computing. IT can provide seamless, instant access to clinical tools while increasing security. Applications and associated patient data remain secure in the data center, where they are accessed through granular, policy-based user authentication. Look for solutions that provide a high-fidelity experience through real-time network and performance optimization, with proven scalability, and that are quick to deploy and easy to use.

Many healthcare organizations have chosen Citrix Workspace to provide on-demand delivery of clinical applications and desktops to any endpoint. This means a near-native experience, even with graphically-intensive imaging applications.

Single sign-on and partner technologies for tap-in, tap-out authentication ensure fast, secure access — reducing log-in times and improving clinical workflows. Compliance with HIPAA and other regulations is supported through behind-the-firewall desktop and application processing; standards-based encryption; secure remote access; password expiry management; enhanced event logging; multifactor authentication; and web application firewall.

With Citrix technology, security is designed around people. People-centric security enables users to seamlessly and securely share information as they collaborate with coworkers and third parties. It includes security analytics that detect anomalies in user behavior that might signal malicious intent or risky behavior. A people-centric approach gives clinicians and healthcare users secure access to apps and data stored in multiple storage zones and promotes user satisfaction by offering a single common interface on any device. As part of that, contextual access limits information access to those who need it, thus providing even more safeguards for sensitive information. A people-centric approach also enables healthcare users to easily access the types of information necessary to comply with HIPAA, MACRA, and other mandates. Security protects information and applications but doesn't stand in the way of productivity.

Another key component of mobility is secure file sharing across the healthcare delivery chain. HIPAA-compliant Citrix ShareFile® lets users securely share lab results, consult notes, medical procedure records, and hospital processes information with any authorized user. It has been certified under the Sword & Shield HIPAA Compliance Program.

Step 4: Select technologies to ensure secure, user-friendly mobility

Some users need more than Windows apps on devices: they want to use native mobile apps alone or in conjunction with corporate apps. Some prefer, or are required to use their own devices. Some even want to mix work-related mobile apps with personal apps on the same device. Your mobility management policy, technology, and security strategy may need to address all these variants.

The technology chosen should separate corporate apps and data from personal content, and provide end-to-end control and protection. The best solutions provide mobile productivity apps, data sync, a secure mobile gateway, and a unified app store. For example, Citrix Endpoint Management is tightly integrated with Citrix Apps and Desktops. It gives users full access to mobile, Windows, web and SaaS applications from a single unified storefront, single sign-on, and a single storage solution. For IT, it provides identity-based provisioning and control of apps, data, and devices. You can enroll and manage any device and control application access through app tunnels, blacklisting, dynamic policies and more. With protection against mobile threats, rogue device blocking and SIEM integration, you can give users freedom of choice in devices while ensuring compliance and patient privacy.

Step 5: Select technologies that provide IT flexibility and control

Healthcare is an industry undergoing constant growth: multi-facility organizations, new facilities and groups, mergers, acquisitions, telemedicine, and more, serve to extend the perimeter and enlarge the user base. To ensure that everyone has access to data and applications, look to secure cloud networking and a front-end that provides granular context-aware policy controls for virtual applications and client resources. A gateway that provides secure remote access should use SSL for all network traffic and include session recording for compliance (and advanced troubleshooting).

Citrix ADC and Citrix Secure Web Gateway offer a unified management framework with load balancing, global traffic management, security, data scaling, app visibility, and desktop delivery to help your organization grow, while consolidating data centers to minimize risk and costs. Access control, auditing, and reporting help you manage compliance, information governance, and data protection. Citrix ADC makes it possible to consolidate critical network services on a single hardware appliance with no loss of performance, and meet diverse application needs in a multitenant environment.

Step 6: Bring it all together for a successful rollout

Develop and implement a rollout plan, including architecting the solution and onboarding users. On the architecture side, Citrix Workspace cost-effectively bundles the Citrix technologies mentioned above into a complete and integrated solution. In the Citrix Workspace architecture in use by many healthcare organizations, mobile users have access to their Windows, applications or full Windows desktops, along with all their other mobile, web and SaaS applications, all from a single pane of glass.

For user onboarding, in parallel with determining the underlying architecture, you will need to create resources that make it simple for stakeholders to learn what they need to get started.

For mobile users, this should include setting up enrollment procedures, providing tools that enable Self-provisioning, and establishing support, and maintenance levels.

Conclusion

These six steps can lead to a successful healthcare mobility initiative, resulting in impressive results. When physicians have seamless, quick access to vital data, they have more time for patient interaction. When IT plans, engages stakeholders, and chooses the right technology, it results in quicker implementation, reduced complexity, and even significant cost savings.

For more information and examples of how healthcare organizations have enabled their clinicians with mobile access to apps and data, visit

https://www.citrix.com/solutions/healthcare/

Additional Resources

Blog: Precision medicine, meet intelligent workspaces

Blog: The 3 Es of computing in healthcare

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States