

Healthcare Mobility Best Practices

Secure, Reliable Connections
for Better Patient Care

INDUSTRY SPOTLIGHT

Healthcare

Overview

Accessing patient data directly at the point-of-care via wireless technologies is a major focus among healthcare providers. In a recent survey of healthcare IT decision makers, 80% reported that mobility initiatives were more important to their organizations than they were a year ago. Applications leading the way included electronic health records (EHR), computerized physician order entry (CPOE) and medication administration. These initiatives drive overall improvements in patient care and new efficiencies. They were associated with a 31 percent reduction in manual errors, and an increase of 39 productive minutes per worker per day. (*Motorola Enterprise Mobility Barometer: State of Mobility in HealthCare*, 2009.)

The flipside, of course, is the mandate to secure data in light of HIPAA/HITECH and other patient privacy guidelines, as well as ensuring that productivity gains are not negated by system complexity. If the technology is difficult or frustrating to use, clinicians whose primary mission is treating patients — not tackling IT issues — will partially comply with using the system, circumvent it or abandon it.

Wireless-Deployment Strategies

On a hospital campus or in outpatient clinics, mobile clinicians typically access data over a wireless LAN through strategically located access points. In the community, home-health workers, emergency-services personnel and other mobile clinicians access data networks using air cards from cellular carriers.

In both scenarios, maintaining continuous connections can be a challenge. Medical centers harbor “dead spots” for coverage such as long hallways, stairwells, elevator shafts and hidden obstructions. Cellular coverage can be spotty due to man-made obstacles, reflective surfaces, varied terrain and tower distribution. When clinicians enter no-coverage zones, the network connection drops, open applications hang or crash, and physicians and nurses are forced to re-log in to the system and may need to re-enter lost data.

Improved Care, Fewer Help-Desk Calls: Mobility XE for Healthcare

NetMotion Mobility XE is a mobile Virtual Private Network (VPN) widely used in healthcare settings. Organizations that have implemented Mobility XE have realized the clinical improvements of bedside data access, while sharply reducing help-desk calls from users. That is because unlike other types of VPNs, Mobility XE is expressly designed for mobile environments. In such environments, workers roam and use computing devices constantly, while expecting uninterrupted use of open applications throughout the workday. Other types of VPNs can handle some of the security requirements, but not the practical mandate to keep clinicians maximally productive and able to focus on their patients.

Here are the fundamentals of how Mobility XE delivers security with a seamless user experience.

Marshfield Clinic Spans Multiple Locations with Seamless Coverage

Wisconsin-based Marshfield Clinic wanted its nurses, medical assistants and more than 800 physicians to be able to access critical applications and images, and update EHRs at the point of care. With 40 hospital, clinic and retirement home locations to cover, they turned to Mobility XE for continuous application access as staff moves between wireless and wired networks. And since Mobility XE encrypts all wireless transmissions and protects networks from unauthorized access, Marshfield no longer worries about the security of its sensitive patient records.

“Mobility was easy to implement... We were euphoric. NetMotion was like a guy on a white horse riding up with a solution. It enabled everything to come together.”
- Tom Bera, Dir. of Clinical Info. Services

Visiting Nurse Service of New York Finds Home for Mobility XE

The nation's largest not-for-profit home-care agency employs more than 3500 home-health clinicians, making more than two million patient visits annually. Tablet PCs communicating over cellular data networks allow real-time access to patient data. To protect confidentiality and eliminate complexity for their workers, they deployed the Mobility XE mobile VPN for a solution that was streamlined and easy to manage.

"Beyond its capabilities to let our clinicians roam across different networks securely, we can also control which websites clinicians access, and we are able to push out anti-virus updates to the remote client devices."
- Randy Cleghorne, Director of IT

Authentication

Mobility XE supports multiple authentication methods and degrees of security:

- Single factor – user name and password
- Two-factor – a combination of something that the user knows (a password) and something that the user has (a smart card, RSA SecurID token, fingerprint verified through a biometric scanner, or user certificate stored on the device)
- Multi-factor – single or two-factor user authentication, combined with separate authentication of the device through a digital certificate

Regardless of the number of factors involved, logging onto the NetMotion Mobility XE mobile VPN is as simple as logging on with standard Windows credentials. When enabled, device authentication proceeds in the background without user intervention. This user transparency is vital in

a healthcare setting where clinicians need to focus on patient care – not on their devices. Administrators may, however, require users to reauthenticate at intervals, or after the device has been automatically suspended after a period of non-use. This can be important for protection against a device that has been set aside and could be picked up by a curious patient or visitor.

Encryption

NetMotion Mobility XE supports FIPS 140-2 validated AES encryption at 128-bit, 192-bit or 256-bit strengths, in keeping with the mandate to protect confidential patient data. It secures the entire connection path, maintaining a continuous encrypted tunnel from the client device in the clinician's hands to the Mobility server in the data center. Regardless of the combination of networks the data traverses – including Wi-Fi, cellular or wired campus networks – Mobility XE safeguards both patients and the healthcare organization.

Application Persistence

Even when network connections are interrupted, as might happen when a physician enters an elevator or an ambulance traverses a tunnel, Mobility XE has the unique ability to maintain both the network session and any open applications. Applications don't lose data even when in the middle of a transmission. Any application that runs on a wired network works in a wireless environment with Mobility XE, including medical records, PACS, physician order entry, medical monitoring, pharmacy, patient registration, scheduling, housekeeping, billing and accounting.

Bell Ambulance Responds to the Call With Reliable Connections

The second-largest provider of ambulance service in the state of Wisconsin employs 200 paramedics and EMTs who respond to nearly 5,000 calls a month. The company has deployed tablet PCs in the ambulances and utilizes software to complete patient care reports, which are then synchronized with dispatch and billing applications. The staff uses Mobility XE to stay connected to critical applications, roam seamlessly between multiple wireless networks, and maintain applications even when moving in and out of wireless coverage areas.

"The goal of our wireless deployment is to provide EMTs and paramedics easy and secure access to patient information and, at the same time, to allow the staff to focus on their primary job, which is patient care."
- Steve Caulfield, Network Administrator

Puget Sound Blood Center Keeps Data Flowing

Deploying 18 mobile vehicles, Puget Sound Blood Center collects blood donations across Western Washington, updating donor information in real-time on the mainframe in Seattle. While their Citrix Access Gateway solution allowed wireless connections via cellular data networks, even a split-second coverage loss meant technicians had to re-log in and diagnose technical issues. Switching to Mobility XE preserves the connection, even in areas that had previously been identified as dead zones for coverage.

“The benefits of Mobility XE are clear. Now our blood technicians can focus on their main function, which is to draw blood, rather than dealing with connectivity issues.”
- Kiefer Atkins, Information Technical Analyst

Internetwork Roaming

When users cross network boundaries and access multiple networks, Mobility XE automatically handles any separate network logins without requiring user intervention. This is especially advantageous when using cellular networks, as coverage is sometimes spotty and organizations often need to employ two or more carrier networks to fully cover their service area. The same seamless roaming applies when using multiple access points on a medical campus.

Policy Management

Policy Management heightens security and productivity by controlling how applications, users and devices access networks. It is possible to allow only specific clinical applications, prohibit Web browsing, only allow access to an intranet or specific clinical sites, or to set restrictions based on connection speed or time-of-day. Tablet PCs used by roaming clinicians, smartphones in the hands of

physicians, notebooks carried by home-health workers and executive laptops can all have different policies, further defined at the user level.

Network Access Control

Integrated Network Access Control (NAC) verifies that devices have required security precautions in place – such as patches, operating system updates, and active antivirus with current signatures – before allowing a connection. NAC integrates with Policy Management to automatically remediate devices, in a way that doesn't interfere with patient-care duties.

Quality of Service

Traffic-shaping capabilities give priority access to network bandwidth to the most critical applications, so that Web browsing or large file downloads don't interfere with the medical mission. Patient monitoring systems or applications that physicians depend on such as point-of-care, CPOE or PACs, may be assigned higher priority than scheduling and billing. Medical centers that employ VoIP devices for push-to-talk communications may single out voice traffic for highest priority to preserve quality.

St. Joseph's Hospital Overcomes Multi-story Coverage Problems

At Wisconsin-based St. Joseph's Hospital, laptops on medical carts and tablet PCs carried by physicians roam throughout the facility, across multiple floors which present numerous transmission obstacles. Mobility XE delivers high-level security, allows access to medical records from anywhere, and sustains applications as clinicians roam in and out of coverage.

“Devices became much more reliable with Mobility. We got lots of positive feedback from nurses... The Mobility VPN gave us one more level of security for patient information.”
- Todd Zieglmeier, IT Manager

Device Management

Managing hundreds of devices deployed throughout a medical center, inside ambulances or carried by roaming home-health workers is difficult, especially when management activities can't risk interfering with clinical duties. Mobility XE allows device management through a central console, and also integrates with enterprise-level management solutions from third parties. The integration allows management chores, such as application updates, to run when users aren't actively logged on, between shifts.

Analytics and Notifications

Monitoring performance across multiple networks is a challenge, especially when those networks are outside of IT's direct control. Analytics report on device and network usage, while notifications alert administrators about problems – often before they reach a threshold that could impact clinicians. This can dramatically decrease help desk calls, and assist in resolving issues before they impact patient care.

For More Information

For healthcare case studies and more information, please visit www.netmotionwireless.com.

© 2010 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPsec, InterNetwork Roaming, Best-Bandwidth Routing and Analytics Module are trademarks of NetMotion Wireless, Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, SQL Server, Windows XP Tablet PC Edition and Windows Vista are registered trademarks of Microsoft Corporation. All other trademarks, trade names or company names referenced herein are used for identification purposes only and are the property of their respective owners. NetMotion Wireless technology is protected by one or more of the following US Patents: 5,717,737; 6,198,920; 6,418,324; 6,546,425; 6,826,405; 6,981,047; 7,136,645; 7,293,107; 7,574,208; 7,602,782; 7,644,171; and Canadian Patent 2,303,987. Other US and foreign patents pending.