Cloudpath

Simple & Secure Mobility in Healthcare

Simple Mobile Security

The advantages of mobile technology in healthcare are numerous and well known. Patient care is improved through immediate access to patient data and reference materials. The patient and visitor experience is improved through the availability of Wi-Fi access.

The response to personal devices in healthcare has centered on mobile device management (MDM). MDM solutions are expensive, require significant infrastructure investments, and fail to address the many rapidly evolving Wi-Fi use cases in healthcare. Restricted to a single MDM domain, physicians and contractors have difficulty working across multiple facilities. Patients are not supported, leaving them to fend for themselves on unencrypted Wi-Fi. Nurses and other support staff, hesitant to accept the heavy management on their own personal device, often bypass policies via 4G or use the guest wireless network.

The Opportunity

69% of clinicians today use mobile technology to view patient data, and patients increasingly expect user-friendly Wi-Fi access. Additionally, facilities increasingly utilize Wi-Fi enabled equipment. With HIPAA compliance as the 800-pound gorilla in the room, the need for a consistent approach to secure Wi-Fi, for all users and all devices, is required.

> "Insist upon open standards-based interoperability for new purchases!"
>
> The West Health Institute and the office of the Nation Coordinator for Health Information Technology 2014

To enable secure Wi-Fi for all users, you need a standards-based, vendor-agnostic approach that is simple, secure and doesn't require a commitment to a proprietary approach. You need a solution that interoperates with your existing architecture, requiring no significant hardware investment, and one that's easy to manage. You need a one-stop mechanism to easily and securely onboard devices while applying the appropriate policy for each user and device. With this, you can focus less on Wi-Fi and more on what's really important: patient care.

The Solution: Automated Device Enablement

Automated Device Enablement (ADE) by Cloudpath Networks provides a simplified approach for deploying certificate-based Wi-Fi to personal devices. Designed for the era of personal devices, ADE allows devices to be assimilated easily, securely, and without IT involvement. Through smart, policy-associated certificates and the wireless standard WPA2-Enterprise, ADE provides visibility and control over personal and IT-owned devices without the need for on-device agents and with broad device support.

The ADE approach is implemented in the XpressConnect Enrollment System (ES). Built upon industry-leading onboarding and certificate management capabilities, the XpressConnect ES:

- Provides automated, self-service onboarding for all users, including employees, physicians, patients, visitors, and contractors.
- Automatically assigns and enforces policy based on the user, device, ownership, and more.
- Automates the distribution of certificates from built-in and third-party certificate infrastructure, including Microsoft CA.
- Automates the configuration of WPA2-Enterprise and wired 802.1X with EAP-TLS.
- Enforces and remediates NAC best practice requirements, including antivirus, firewalls, screen locks, and system updates.
- Supports a broad array of devices, including laptops, tablets, phones, and headless devices such as printers, cameras, VoIP phones, and barcode scanners.

83% of healthcare organizations indicate physicians at their organization use mobile technology to facilitate PATIENT CARE.

Third Annual HiMSS Analytics Mobile Technology Survey

- Provides onboarding options for various use cases, including BYOD, guest sponsorship, secure hotspot, and time-limited access.
- Provides visibility into users, devices, and policy assignment and per-device control over access rights.

In brief, the XpressConnect ES automates the operation of a certificate-based WPA2-Enterprise wireless network, or a wired 802.1X wired network, leading to a better user experience and reduced support costs.

XpressConnect ES allows you to:

- Provide encrypted Wi-Fi to physicians using gold-standard security in a manner that allows roaming between facilities.
- Provide patient and visitor access that is secure and elminates the annoyances of repeated web logins.
- Provide secure BYOD Wi-Fi access to staff that prevents bypassing policies via external networks.
- Enable WPA2-Enterprise security on IT-owned medical equipment, eliminating the security and manageability issued of pre-shared keys.

Using your existing WLAN infrastructure, XpressConnect ES enables quick, easy and secure access to more users and more devices while reducing support costs and ensuring policies are appropriately enforced.