Adventist Health System Redefines Clinical Workflows on Mobile Devices to Improve Patient Care
Adventist Health System Redefines Clinical Workflows on Mobile Devices to Improve Patient Care

Mobility has the power to give caregivers the information they need sooner and ultimately change patient outcomes for the better. In fast-paced healthcare environments, access to patient records and clinical information on mobile devices can make a critical difference. But providing that access is not always simple – healthcare facilities are bound by federal regulations to protect electronic patient health information that is accessed or transmitted on mobile devices. Securing these mobile devices is imperative to protect patient privacy and avoid data loss.

The Adventist Health System is working to improve clinical workflows while ensuring data security by providing employees access to email and clinical information on AirWatch-managed mobile devices. The Adventist Health System IT department provides secure access for more than 7,000 employees on iOS and Android devices. AirWatch® provides oversight and security to help the IT department ensure its employees maintain regulatory compliance. For example, AirWatch® Mobile Email Management ensures that emails remain encrypted and can only be accessed by compliant devices that are enrolled in AirWatch® Mobile Device Management. Additionally, AirWatch® Secure Content Locker® ensures attachments can only be opened in an encrypted container and that no information is stored in unsecured apps.

Working closely with stakeholders across departments, the Adventist Health System IT department is deploying a variety of mobile technologies that make it easier for caregivers to access clinical data, while ensuring the organization maintains compliance. These efforts ultimately result in improved workflows that facilitate better patient care.

Adventist Health System demonstrates the following four best practices for implementing a mobility strategy that provides mobile access and ensures compliance, efficiency and productivity for all stakeholders.

Managing Different Deployment Models in a Single Console

The IT department at Adventist Health System was recently faced with a pressing question: “How do we handle the growth of personal devices within our organization?”

“Some employees have two or three devices, and many upgrade quickly to the latest devices, meaning IT has to manage a constantly widening stream of devices,” says Brent Snyder, CIO for Adventist Health System.

Prior to 2010, Adventist Health System had managed an all-BlackBerry deployment providing BlackBerry Enterprise Server (BES) 5 to all eligible employees. The rise in popularity of smart phones, and financial benefits to moving toward an employee-provided device program, prompted the organization to purchase a second enterprise mobility tool, a sandboxed solution that would enable secure email delivery and management of employee-owned devices. But managing devices across multiple systems quickly became challenging. Each needed its own system administrator who understood the console and the devices managed therein.

“We struggled to provide the usability features requested by employees,” said Herb Keller, chief technology officer for Adventist Health System. “We saw an opportunity to use AirWatch Mobile Device Management to provide a more native user experience with iOS and Android devices.”
Adventist Health System's IT department was drawn to AirWatch for its single pane of glass management, which enables efficient management of all devices, regardless of manufacturer or operating system. Having a birds'-eye view of all devices in the deployment would also help Adventist Health System identify security threats more quickly than would have been possible with multiple systems to maintain. AirWatch also had the potential to help with some of the feature requests the IT department was getting. Rather than just secure access to email, AirWatch opened the door for Adventist Health System to enable doctors, nurses and hospital staff to access relevant content and applications more securely.

**Enabling Clinicians with Secure Access to Content and Email**

Adventist Health System employees needed secure mobile access to the health system’s Exchange ActiveSync email server. But data security requirements prohibited setting up native access to ActiveSync on employee-issued devices without additional security in place. Adventist Health System needed an email solution that would enable the IT department to apply root detection, prevent data from being stored on devices, and control attachments, all while providing users a native experience.

After enrolling devices in AirWatch Mobile Device Management, the Adventist Health System IT team set up AirWatch Secure Email Gateway to secure email transmission. AirWatch Secure Email Gateway provides a way to rewrite and encrypt all attachments sent via email, which can contain protected health information. Now, employees enrolled in AirWatch have access to email through their device’s native client, and administrators have the controls required by their data security office and federal compliance regulations.

To control how attachments were opened and shared, the team pushed the mobile content management solution AirWatch Secure Content Locker to devices. Using AirWatch, administrators set a profile that ensured attachments could only be opened in Secure Content Locker®, an encrypted container, and that no data was stored on the device. The solution works for both organization- and employee-owned devices. Now, when devices are lost or an employee leaves the company, all protected information, including content in Secure Content Locker, can be removed by an IT administrator without affecting personal data on employee-owned devices.

Adventist Health System clinicians can now use the solution to collect patient signatures on relevant forms right at the bedside. Using hand held tablets creates a more efficient and mobile work environment for the clinicians. Doctors and nurses also use AirWatch-managed iPads to track hospital bed availability and enable patients to complete surveys at the bedside. Adventist Health System anticipates working with its EMR vendor to build upon these current initiatives to provide more efficiency advantages using mobile devices across its more than 40 hospital campuses in ten states. “As clinicians begin to realize how they can improve patient care with mobile devices, requested use cases are growing by the day,” Keller says.

**Security and Regulatory Compliance**

To meet the requirements of the HIPAA Security Rule and help prevent data breaches on mobile devices, HHS recommends that healthcare organizations analyze risks, identify points of a potential data breach and take certain steps to protect data.

According to HealthIT.gov, the HIPAA Security Rule requires covered entities to “maintain reasonable and appropriate administrative, technical and physical safeguards for protecting e-PHI transmitted on mobile devices.” By selecting AirWatch, Adventist Health System IT administrators are able to enforce each of the following parameters, as recommended by HHS: Use a password; install and enable encryption; install and
activate remote wiping and/or remote disabling; disable and do not install or use file sharing applications; install and enable security software and keep it up to date; research mobile applications before downloading; maintain physical control; use adequate security to send or receive health information over Wi-Fi networks; delete all stored health information before discarding or reusing the mobile device, and ensure and maintain compliance of end users.

To learn more about how AirWatch helps healthcare organizations like Adventist Health System meet these recommendations, read the AirWatch white paper: “Protect and Secure Patient Data on Mobile Devices: Support HIPAA Compliance,” which is available for download on the AirWatch Resources page.

**BYOD**

To enable employees to bring their own devices to work, Adventist Health System created a process by which employees have their choice of device, and once registered in AirWatch Mobile Device Management, can rest assured that their personal information will be kept private.

AirWatch offers two options for securing BYOD devices: AirWatch Mobile Device Management or containerization with AirWatch® Workspace. AirWatch supports all major mobile platforms, allowing organizations to implement flexible BYOD programs. Employees can choose from the latest makes and models for their smartphones, tablets and laptops. Administrators can define devices eligible for enrollment with custom device whitelists and blacklists.

AirWatch Workspace has helped the Adventist Health System IT department create a more consistent user experience across a wide range of BYOD device types. “Android has so many hardware manufacturers that the experience can be inconsistent,” Keller says. But AirWatch Workspace “allows us to deploy management products at the operating system level.” The Adventist Health System IT department is in the process of migrating about 500 Android devices to AirWatch BYOD management.

AirWatch’s simple enrollment process has also enabled IT administrators to provide a consistent enrollment experience for BYOD users across device types. Once users are authenticated, profiles, applications and content that have been designated by the Adventist Health System IT department are configured automatically based on the user and device ownership type. Adventist Health System IT administrators can provide employee-owned device connections to intranet sites and organizational content, email apps, Wi-Fi, VPN networks and more from their mobile devices by pushing profiles automatically or on demand. From the AirWatch self-service portal, employees can enroll additional devices, view detailed device information and perform remote actions.

**Additional Resources**

For additional information, visit [www.air-watch.com/industries/healthcare](http://www.air-watch.com/industries/healthcare).

For more information about Adventist Health System’s AirWatch deployment, read the [case study](#).

To get started with a free trial of AirWatch, visit [www.air-watch.com/free-trial](http://www.air-watch.com/free-trial).