Improve Patient Care and Revolutionize Healthcare with Mobility: Best Practices
Improve Patient Care and Revolutionize Healthcare with Mobility: Best Practices

In healthcare, mobility initiatives must strike a delicate balance of security, access and ease of use. In fast-paced clinical environments, caregivers need a simple way to access data at the point of care. Mobile access to data has the power to provide caregivers with the information they need sooner and change patient outcomes for the better. IT departments, on the other hand, must adhere to healthcare’s strict regulatory environment when designing a mobility strategy. This white paper outlines best practices for designing and implementing a mobility strategy that facilitates mobile access to real-time clinical data while ensuring compliance, efficiency and productivity.

Managing Your Mobility Strategy

IT departments are constantly inundated with new feature requests, helpdesk tickets and security threats. When developing and maintaining a comprehensive mobility strategy, it is important to consider the added burden that will be placed on the IT department. A manageable, effective enterprise mobility management (EMM) solution needs to be simple to set up, implement, manage and scale as more devices and use cases develop. Enterprise mobility management solutions from AirWatch provide a single pane of glass through which administrators can easily and efficiently monitor, maintain and secure all devices in a healthcare deployment.

AirWatch offers comprehensive enterprise solutions to enable doctors, nurses and hospital staff to access relevant content, email, applications and secure browsing in a single EMM solution, built from the ground up with security at the core. Through delegation of administrative control, a self-service portal and automated processes, AirWatch enables IT administrators to manage mobility efficiently.

AirWatch enables IT departments to delegate responsibilities to different individuals throughout an organization through role-based administrative control. IT departments can simplify what an administrator sees when he or she logs into the console so that only the most pertinent information is displayed to that individual. For instance, the IT administrator can delegate limited administrative responsibilities to department heads, so the person who is directly responsible for a group of employees also controls what content and applications they access.

The AirWatch self-service portal cuts down on helpdesk calls by enabling end users to solve problems related to their devices. From the portal, employees can enroll additional devices, view detailed device information and perform remote actions.

The AirWatch compliance engine is an automated policy enforcement tool that administrators can leverage to maintain pre-defined rules for mobile devices. Through the use of profiles, administrators can configure compliance policies that trigger escalating actions when a device is detected as noncompliant. Examples of noncompliance include attempting to root or jailbreak the device or downloading a blacklisted application. AirWatch provides 24/7 device monitoring, and administrators can be notified by email when a device leaves compliance and an action has been triggered by the compliance engine.
AirWatch also provides educational resources for IT staff tasked with maintaining a mobile deployment. MyAirWatch is a portal that provides relevant information such as product documentation, training videos, articles and forums to help support AirWatch administrators. AirWatch also offers Associate and Professional Certification programs, which certify administrators and enable them to use AirWatch to its full potential.

**Staff Training and Enrollment**

To ensure a seamless transition to managed devices, consider hosting an on-site enrollment event. Have IT staff members on hand to walk employees through the enrollment process and answer questions. IT staff can also demonstrate the self-service portal, from which employees can enroll additional devices, view detailed device information and perform remote actions. Users can see installed profiles and applications, view GPS location (if enabled), query the device and clear passcodes. Users can also make requests for apps, profiles and technical support through the portal. These capabilities significantly reduce IT helpdesk burden.

AirWatch’s automated enrollment empowers employees to enroll and manage their own devices. To enroll, users simply navigate to a URL that IT provides and enter their credentials.

Enrollment is further simplified for organizations that choose to organize their mobile deployment using existing directory settings. AirWatch securely integrates with AD/LDAP, certificate authorities, email infrastructures and other enterprise systems both in cloud and on-premise deployment models. For cloud deployments, AirWatch integrates your cloud instance to your on-premise services through a secure, self-service process directly from the AirWatch console. For on-premise environments deployed in tiered network models, AirWatch can be set up to communicate to various facility services across network layers. Integrating with an existing directory allows users to enroll with their existing credentials. The integration will also automatically group users based on directory groups.

**Regulatory Compliance**

To meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and help prevent data breaches on mobile devices, the U.S. Department of Health and Human Services (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 electronic protected health information (ePHI) transmitted on mobile devices.” HHS recommends taking the following steps to protect patient data and prevent data breaches: 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 a firewall; 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 can help healthcare organizations meet these recommendations, read the AirWatch white paper: “Support HIPAA Compliance: Protect and Secure Patient Data on Mobile Devices,” which is available for download on the AirWatch Resources page.

Managing Different Deployment Models

Facility-owned Devices

Facility-owned devices can be used to enable doctors, nurses, hospital staff and even patients with access to information and resources. Facility-owned devices are helping doctors communicate with experts that are thousands of miles away. Mobility provides an inexpensive alternative to traditional telemedicine, if the devices are managed and secured appropriately.

With AirWatch, administrators can manage all deployment models from a central console. AirWatch’s multitenant architecture is designed to support a large number of devices, and scale as a healthcare organization expands its mobility initiatives. Administrators can manage all devices across locations in a single console. The entire device fleet can be managed at a global level while empowering different groups or divisions to maintain visibility and control of devices.

Many healthcare organizations choose to start their mobility initiatives with dedicated devices owned by doctors and full-time staff, and add shared devices for hourly employees and patient-facing devices later. The AirWatch solution enables administrators to enroll devices quickly, configure and update device settings over the air and secure mobile devices. With AirWatch, administrators can manage a diverse fleet of Android, Apple iOS, BlackBerry, Mac OS, Symbian, Windows Mobile, Windows PC/RT and Windows Phone devices from a single management console. For all ownership models, healthcare organizations can give corporate employees secure access to email, calendar, contacts, apps, content and more.

Shared Devices

AirWatch provides a multiuser management solution that meets enterprise security and management requirements for corporate devices, while providing the personalized experience users demand. The AirWatch shared device feature enables administrators to seamlessly provision a single managed device with settings and features specific to multiple predefined user roles. For example, a nurse on a morning shift can check out a device and access material that is unique to him or her. At the end of the shift, the nurse can check in the device, setting the device back to a blank, unassigned state, while still under management. The AirWatch shared device feature is integrated within the AirWatch® Agent to ensure the most streamlined user experience. It does not require re-downloading of apps or re-provisioning of the device, so there are no gaps in management, and the device is always locked down and secured.

For shared devices, administrators can import authentication information for their employees by syncing with existing back-end systems. Device-level authentication will enable healthcare organizations on a budget to use the same device for multiple purposes and/or user types. In some cases, a single device will be assigned to a nurse station. Other organizations are giving each nurse on duty a shared device that can be used to remotely monitor each patient under the nurse’s care. The tablets can be used to keep an eye on all patients at once, access detailed patient information and record data at the point of care.
BYOD

AirWatch offers two options for securing bring your own device (BYOD) deployments: 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’s simple enrollment process provides a consistent agent-based flow for major platforms. Once users are authenticated, profiles, applications and content are configured automatically based on the user and device ownership type. AirWatch enables secure access to enterprise resources from employee-owned devices. Administrators can provide employee-owned devices connections to intranet sites and organizational content, email apps, Wi-Fi, virtual private networks (VPN) 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.

To protect BYOD users’ privacy, administrators can create customizable privacy policies based on device ownership type. AirWatch recommends that organizations create BYOD policies that clearly define that only organizational data can be accessed. Administrators can then configure policies to prevent data collection from personal email, content or applications on an employee-owned device. GPS location, personal user information and telecom data can also remain private, and employee-owned devices can be protected from a full device wipe or remote control.

AirWatch also allows businesses to mitigate risks that are presented when employee-owned devices are accessing organizational resources. With custom terms of use agreements based on user role, organization group and device platform, users can be informed about data that will be captured and what they are allowed to do with the device.

AirWatch also offers an alternative to MDM with AirWatch Workspace, an applications-based approach to securely accessing organizational data. AirWatch Workspace is a container that houses AirWatch and organizational apps on a device, enabling secure access to data – including email, applications and content, as well as a secure browser – on devices that are not managed with MDM. Rather than managing the entire device with MDM, AirWatch Workspace provides a managed space on employee-owned devices, which some organizations feel better suits their policies.

Available on both iOS and Android devices, the containerized solution is ideal for BYOD initiatives and for extended enterprise collaboration. Containerization can be a good option for Android-heavy BYOD environments. AirWatch Workspace provides a consistent user experience across all versions of Android, regardless of the device manufacturer. Some organizations are deploying MDM and AirWatch Workspace on the same device, for an added layer of security.

Considerations for Acute Care Deployments

Patient-facing Devices

Supervised mode and kiosk mode are valuable tools for patient-facing devices. Apple iOS devices that have been enrolled and staged with Apple Configurator can be used as customer-facing devices in supervised mode, which enables administrators to lock devices into a single app, such as AirWatch Browser. The same
features are available for Android devices through the AirWatch® Secure Launcher for Android.

Healthcare organizations are using these features to lock a kiosk device in a waiting room into a check-in app. Others are using kiosk devices for in-room entertainment, check-out paperwork, or to entertain children in waiting rooms with an approved list of gaming apps.

Preparing Your Hospital Network

As a best practice, AirWatch recommends that healthcare facilities set up two Wi-Fi networks: One secured network for employees and a separate public network for patients and visitors. Within the AirWatch console, administrators can limit Wi-Fi connection on managed devices to the secured network, so hospital devices cannot access the public Wi-Fi network. To ensure the security of the private network, AirWatch partners with network access control providers. Network access control can detect any new or unmanaged devices that attempt to join the secure network and redirect them to the AirWatch Agent or enrollment URL to enroll (or re-enroll) a device. This ensures that the IT administrator has oversight for all devices accessing the secure network.

AirWatch is in the process of creating a solution to allow healthcare organizations to leverage distributed nodes over hospital networks. Individual locations will be able to host content received from the central AirWatch server and then deploy that content to devices in the same network. This method of content distribution will significantly reduce bandwidth load.

AirWatch recommends that IT administrators test Wi-Fi connectivity for mixed devices in various locations and consider the clinical impact of network outage.

Managing and Deploying Applications

With AirWatch, administrators can manage the entire application lifecycle, from testing through deployment, updates and retirement. Administrators and developers can test applications in AirWatch through a controlled release, which enables deployment to a control group to test for issues before widely deploying the app. AirWatch offers application versioning, which enables IT administrators to require application updates – this can be done organization-wide or through a phased roll out.

Administrators can make applications available to users through the AirWatch® App Catalog, a custom app catalog for your facility where employees can access and download both internal and third-party applications that are managed with AirWatch. Apps for accessing EMRs, scheduling, insurance information and more can be uploaded into the AirWatch console and pushed down simultaneously to specified devices. Apps can be distributed based on smart groups, which can be based on location, job function or other variables.

Managing Secure Access to Resources and Content

With AirWatch, administrators can provide access to content repositories and enterprise networks by configuring certificate-based authentication to a VPN. With VPN profiles, administrators can allow employees to connect to enterprise VPN networks on their mobile devices without user interaction. AirWatch enables IT administrators to push VPN profiles automatically or on demand and assign based on user group, location or time of day. For example, IT administrators can set a defined geofence for a VPN profile to be active. If an organization wants BYOD devices to access hospital networks only while on hospital grounds, a geo-fence profile will automatically disable access when the device leaves the premises.

VPN On Demand allows mobile users to securely access specific websites through a VPN tunnel. This process
is invisible and seamless to the user, allowing them to continue working without interruptions. This feature is useful for doctors who travel from facility to facility, or for remote care workers who still need access to hospital resources.

**AirWatch® Secure Content Locker™** can also provide users with a central application to securely access patient records, medical images and other documents from their mobile devices. End users are authenticated using AD/LDAP, Kerberos, token-based or certificate-based methods before gaining access to Secure Content Locker. All data and content sent to mobile devices is encrypted in transit and at rest with AES 256-bit, FIPS 140-2 compliant encryption. Access control lists can be used to assign content at the corporate, organization group and user level to ensure users only access the right content. Permissions are configurable for sharing, offline viewing, third-party app access, emailing and printing on a per document basis. If used in conjunction with AirWatch Mobile Device Management, AirWatch can continuously monitor devices for compliance and revoke access for noncompliant devices.

**Considerations for Remote Care Deployments**

**Managing and Deploying Applications**
As with on-site workers, administrators can maintain full application management on the devices of healthcare workers in the field. In home healthcare scenarios, AirWatch administrators can ensure that workers are able to access relevant content and applications on the go from their device without compromising security. With AirWatch, administrators can push down billing and record keeping applications for field workers.

**Managing Secure Access to Content and Email**
With Secure Content Locker, remote healthcare workers can have anytime, anywhere access to their organizational content and patient health records. AirWatch offers two options for giving remote employees access to email: through the use of the device's native email client or through AirWatch® Inbox, a containerized email solution. With AirWatch® Mobile Email Management, administrators can enable features such as attachment stripping, hyperlink stripping and open-in restrictions, which limit users to opening hyperlinks and attachments into approved and secure applications.

Through VPN On Demand, AirWatch provides the ability to provision a VPN profile to devices to automatically configure access to facility networks and file systems. VPN On Demand allows mobile users to securely access specific websites through a VPN tunnel. This process is invisible and seamless to the user, allowing them to continue working without interruptions. VPN On Demand is useful for doctors who travel from facility to facility, or for remote care workers who still need access to hospital resources.
Additional Resources

For additional information, please visit www.air-watch.com/industries/healthcare.

To get started with a free trial of AirWatch, visit www.air-watch.com/free-trial.

AirWatch Global Headquarters
1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch
AirWatch is the largest Enterprise Mobility Management provider in the world with over 1,600 employees globally. More than 10,500 companies trust AirWatch to secure and manage their mobile enterprise. With market-leading solutions for mobile security, device, email, application, content and browsing management, we simplify enterprise mobility.