Adventist Health System Delivers Premium Patient Care with AirWatch-managed Devices

The Client

Adventist Health System is a faith-based health care organization headquartered in Altamonte Springs, Florida. Adventist Health System's more than 70,000 employees maintain a tradition of whole-person health by caring for the physical, emotional and spiritual needs of every patient.

With 45 hospital campuses and nearly 8,300 licensed beds in 10 states, Adventist Health System facilities incorporate the latest technological advancements and clinical research to serve more than 4.5 million patients annually. The full continuum of integrated care also includes urgent care centers, home health and hospice agencies, and skilled nursing facilities. Each Adventist Health System facility operates independently in delivering care and services to best meet the needs of the local communities they serve.

Solution Overview

- Client: Adventist Health System
- Industry: Healthcare
- Geography: North America
- Features: BYOD, Workspace, MDM, MAM, MCM, MEM
- Infrastructure Integrations: Active Directory, SharePoint, Exchange, Certificate Services, File Shares, Office 365
- Devices: 1,000 – 5,000

The Challenge

Adventist Health System had been searching for a way to incorporate mobility into its employees' workflow to enable them to perform their jobs more efficiently and securely. As email became a major communication method for employees, the healthcare organization deployed multiple legacy systems to manage corporate-owned and personal devices for secure email access. However, access to corporate resources and device management capabilities were lacking for the robust security needs of Adventist Health System. "Our legacy systems were limited to email access," said Mark Dunkerley, enterprise technical solutions engineer, Adventist Health System. "We struggled to provide the usability features requested by employees."

Adventist Health System also required patient records to be secure within the hospital environment as they continue to move to digitized private health information (PHI). With the growth of mobile usage and demand from users, the healthcare organization is being challenged with providing access to this digitized information through mobile devices in a secure manner while complying with HIPAA regulations and maintaining patient confidentiality. To achieve its goals, Adventist Health System outlined four main objectives for a successful management system: Email attachment control; support for a personal identification number (PIN); the enforcement of compliance (jailbreak and root) detection; and an enterprise wipe feature for lost or stolen devices.

+1 404.478.7500 | info@air-watch.com | air-watch.com

The Solution

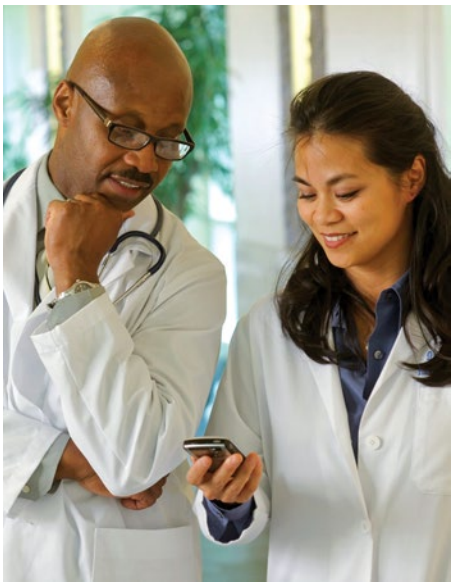
After consulting leading industry reports and testing multiple mobility vendors, Adventist Health System selected AirWatch® by VMware® to replace its legacy systems. To secure email and email attachments, the healthcare organization's technical teams use AirWatch® Secure Content Locker®, a secure content management solution, along with the AirWatch® Secure Email Gateway™. "With AirWatch, we can provide secure email to devices while enforcing encrypted attachments," explained Dunkerley. "We can also configure attachments to only open in AirWatch Secure Content Locker, further protecting sensitive information from going outside a safe environment."

Adventist Health System also deploys corporate-owned devices for day-to-day medical use in its hospitals. Doctors and nurses use AirWatch-managed iPads to track hospital bed availability, complete patient surveys and capture patient signatures. "AirWatch increases our employee efficiency and ease of use for taking care of our patients," said Dunkerley. "As our employees recognize what they can do with these devices, we are starting to see a growing demand for more uses in the workplace."

To keep devices secure and in compliance with regulations, Adventist Health System uses device restrictions, compliance policies and enterprise wipe features enabled by AirWatch. The technical teams require a secure PIN for every device that has access to hospital credentials and records. Adventist Health System also uses the robust AirWatch Compliance Engine to protect hospital assets if devices are jailbroken or rooted, thus maintaining important regulatory security. Additionally, when devices are lost or an employee leaves the company, all protected information, including content in AirWatch Secure Content Locker, can be removed by an IT administrator without affecting personal data on employee-owned devices.

"AirWatch increases our employee efficiency and ease of use for taking care of our patients. As our employees recognize what they can do with these devices, we are starting to see a growing demand for more uses in the workplace."

– Mark Dunkerley
Enterprise Technical Solutions Engineer, Adventist Health



Up Next

The Adventist Health System technical teams are currently exploring using AirWatch-managed iPads for in-patient convenience, including loading devices with games and social networking sites for entertainment while patients receive treatment. For security, a device wipe will be performed on devices when patients are finished using them, giving the next patient a fresh iPad without exposing PHI.

+1 404.478.7500 | info@air-watch.com | air-watch.com