Support HIPAA Compliance:
Protect and Secure Patient Data on Mobile Devices
Support HIPAA Compliance:
Protect and Secure Patient Data on Mobile Devices

More than 7 million patient health records were breached in 2013 alone. For more than a third of the incidents leading to those breaches, the loss or theft of an unencrypted laptop was to blame, according to Redspin’s 2013 Breach Report. The U.S. Department of Health and Human Services (HHS) has listed more than 800 breaches on its website’s “wall of shame” since the HIPAA breach notification rule, which requires organizations to report breaches, became effective in September 2009.

The rule is designed, in part, to help healthcare organizations identify the most common ways breaches occur so they can learn from others’ mistakes. While the industry can certainly benefit from increased transparency, publicly reported breaches can attract unwanted media attention, damage the public perception of a healthcare facility and lead to substantial fines. In 2013, 61 percent of U.S. healthcare institutions reported a security-related incident, leading to $1.6 billion in fines, according to Government Health IT.

In the strictly regulated healthcare industry, it is necessary to take a proactive approach. Today’s healthcare IT departments are charged with identifying breach risks and plugging potential data leaks before they occur. Implementing basic security measures, such as installing and enabling encryption, is a good first line of defense that could have reduced 2013 breaches by more than 30 percent. But securing mobile devices that touch electronic protected health information (ePHI) requires more than basic security, according to the HIPAA Security Rule’s mobile device privacy and security recommendations.

According to HealthIT.gov, the HIPAA Security Rule requires covered entities to “maintain reasonable and appropriate administrative, technical and physical safeguards for protecting ePHI transmitted on mobile devices.” According to HHS, covered entities must take the following steps to comply with the rule:

- Ensure the confidentiality, integrity and availability of all ePHI they create, receive, maintain or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce.

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.

To analyze risks, healthcare organizations should first identify how ePHI will be used on mobile devices. Being aware of all of the ways users will access, store or transmit ePHI is the first step in protecting it. Organizations should then identify risk areas for each unique use case. According to HealthIT.gov, there are three ways in which mobile devices touch ePHI: data access, data storage and data transmission. The AirWatch® Enterprise Mobility Management Platform protects data at each stage.

The following are HHS’s recommendations for securing ePHI on mobile devices. This whitepaper is designed to explain how AirWatch® can help healthcare organizations meet these recommendations, remain HIPAA compliant and ensure patient information is protected.
Use a Password

HHS recommends using “a strong password” that is at least six characters in length and includes a combination of upper and lower case letters, as well as a number and a keyboard character.

AirWatch utilizes configuration profiles to automatically enforce passcode policies on devices. Administrators can assign configuration profiles to devices based on organization group, device model, operating system, ownership, and other attributes. With AirWatch, administrators can require complex passcodes, setting the required length to a specific number of characters.

HHS recommends changing your password at least quarterly. Administrators can also set password expiration and require users to reset passcodes automatically after a certain specified period of time.

HHS also recommends enabling a time out or automatic logoff feature so a device is not left unlocked, and if a device is lost or stolen, someone would need to know the passcode to unlock and use the device. The AirWatch auto lock feature can automatically lock the device after a specified period of time. Administrators can also set a maximum number of failed attempts, which allows them to set a number of failed passcode entries allowed before the device erases all data.

Through the use of encrypted containers, AirWatch also enables administrators to require dual authentication. One passcode entry is required to unlock the device. Administrators can then implement AirWatch container solutions, which require another to access email (AirWatch® Inbox), documents (AirWatch® Secure Content Locker™) or all enterprise data housed in the secure AirWatch® Workspace container.

Install and Enable Encryption

After creating passcode requirements, the next logical step is installing and enabling encryption. HHS recommends that data stored locally on mobile devices and data that is sent and received by mobile devices is protected with government-grade FIPS 140-2 encryption. AirWatch protects data in transit and at rest through the use of application security and containerization technologies: AirWatch Inbox, an encrypted container for email; AirWatch Secure Content Locker, an encrypted container for documents; and AirWatch Workspace, an encrypted container that can house all enterprise applications.

AirWatch also enables administrators to leverage the native encryption features that are built into device operating systems. Administrators can ensure that device-level encryption is always on through pre-set policies and continuous monitoring by the AirWatch compliance engine.

Application Encryption

With AirWatch® App Wrapping, application access can be restricted. Data is secured at-rest with data encryption and in-transit with AirWatch app tunnelling capabilities. Data loss prevention (DLP) restrictions can also be applied to prevent copy/paste, printing, screen capture, Bluetooth and opening files in other applications. Administrators can restrict access to an app based on network connectivity like cellular connection or roaming status. Administrators can wipe local app data and block app access completely if a device is compromised. Administrators can also enable a simplified user experience with single sign on user authentication that will give users access to all managed apps. For organizations that develop and deploy their own apps, the AirWatch® Software Development Kit can be built into the application to provide the same security features.
Email Encryption
AirWatch Inbox is a secure, containerized email client providing complete separation of enterprise and personal data. Protected with AES 256-bit encryption, AirWatch Inbox is configured with advanced data loss prevention policies to secure sensitive data. AirWatch Inbox provides a seamless user experience for quick access to organizational email, calendar and contacts on Android and Apple iOS devices. Ideal for high regulation deployments and BYOD programs, AirWatch Inbox can be deployed as a managed application on the device or within the AirWatch Workspace.

Content Encryption
With AirWatch, administrators can provide access to content repositories and secure mobile communication with enterprise networks by configuring certificate-based authentication to a Virtual Private Network (VPN) or secure Wi-Fi network.

Secure Content Locker protects sensitive content in a container and provides 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. Available restrictions include offline viewing restrictions; preventing cut/copy/paste, printing and emailing; and ‘open in’ restrictions to prevent content from opening in third-party applications. Geofencing can further protect content by removing it from a device when the device leaves a defined area. For complete DLP across enterprise applications, Secure Content Locker can be utilized in conjunction with AirWatch Inbox and AirWatch Browser, as well as other application containers. Links clicked from Secure Content Locker can be made to open in AirWatch Browser, and email attachments can be required to open in Secure Content Locker. Secure Content Locker, in conjunction with the AirWatch® Secure Email Gateway, can encrypt corporate attachments with a unique encryption key, only allowing the email attachments, when on the device, to be opened in the encrypted container. If used in conjunction with AirWatch® Mobile Device Management, devices can be continuously monitored for compliance and access can be revoked for noncompliant devices.

Install and Activate Remote Wiping and/or Remote Disabling
HHS recommends installing and activating remote wiping and/or remote disabling. Both are possible with AirWatch. Through the AirWatch compliance engine, AirWatch can automatically disable access and wipe data if a device is compromised or found to be non-compliant. If a noncompliant device is detected, escalating actions that the administrator has preconfigured are performed automatically to restrict access and prompt the user to bring the device back into compliance. Administrators can limit access to email, data or Wi-Fi, or send an email to a designated third party, such as the device owner’s supervisor. Administrators can specify that if a device remains noncompliant after a certain period of time, the device will automatically be wiped. If a device is reported as lost or stolen, or an employee leaves the organization, administrators can trigger an enterprise-level or device-level wipe remotely from the AirWatch console.

Administrators can also integrate AirWatch with System Information and Event Management (SIEM) solutions for enhanced logging of device and console events. Event logging settings can be configured based on...
severity levels, with the ability to send specific levels to external systems via Syslog integration. Integrating with SIEM solutions can help ensure security and compliance with regulations and organizational policies.

**Disable and Do Not Install or Use File Sharing Applications**

HHS recommends disabling the use of file sharing applications. According to HealthIT.gov, “If you disable file sharing, you reduce a known risk to data on your mobile device.”

It is likely that a certain number of users at any organization are already using consumer file sync and share services. While the familiar user interfaces of these tools are convenient and appealing to the user, most of them lack the software APIs, security and compliance features that are necessary for preventing data loss. Data and documents that are stored in these services are outside the organization’s IT control and will remain in the employee’s personal account even after he or she leaves organization. Using AirWatch MDM, administrators can blacklist consumer file sync and share applications and any other applications that have been deemed security threats.

AirWatch Secure Content Locker provides a secure, enterprise alternative to consumer file sync and share services. With Secure Content Locker, administrators can manage and monitor access to content across all devices from a central console.

**Install and Enable Security Software and Keep It up to Date**

HHS recommends installing and enabling security software on mobile devices and keeping that software up to date. While many consumer mobile security software options exist, an enterprise-grade solution offers far more controls. Using AirWatch allows an administrator to verify that all devices are secured and under management, and to maintain oversight of all devices accessing sensitive information. Administrators can prompt users to enroll in AirWatch, automatically push software updates or prompt users to perform updates and monitor compliance.

**Research Mobile Apps Before Downloading**

Mobile applications used in healthcare are subject to unique guidelines and regulations, especially those that access, store or transmit ePHI. It is integral for organizations to adequately research and test all applications on a device intended for hospital use. AirWatch® App Reputation Scanning enables IT administrators to evaluate the safety of applications, assigning each scanned application a risk profile. In addition, AirWatch partners with application risk management providers [Appthority](https://www.appthority.com), [Veracode](https://www.veracode.com) and [Lacoon](https://www.lacoon.com).

With AirWatch App Reputation Scanning or partner technologies, administrators can identify risky applications and add them to a blacklist, which prevents end-users from downloading them and prompts their removal through escalating actions triggered by the AirWatch compliance engine. For a more direct approach, IT administrators can add only tested and approved applications to a whitelist, which blocks all other application downloads. Whitelists are ideal for highly secure, facility-owned devices.
Maintain Physical Control

HHS recommends that users and organizations maintain physical control of devices at all times. AirWatch dashboards give administrators a real-time, comprehensive view of all managed devices in a deployment. From the dashboards, administrators see a high-level graphical view of their deployment, view a comprehensive list of enrolled devices and drill down into device and user information details. The AirWatch console gives administrators the ability to track the physical location of devices (if location services are enabled) and take action when a risk is detected. Administrators can send commands on-demand to devices to request information and perform actions. Commands include device query, clear passcode, send message, lock device, find device, set roaming, remote view, sync device and perform an enterprise or device wipe. If physical control is ever compromised, administrators can remotely lock or wipe the device to ensure data on the device is secure.

HHS recommends devices should be properly secured when not in use. This includes requiring proper passcode policies, limiting the time a device stays open without locking and locking the device away when necessary.

Use Adequate Security to Send or Receive Health Information Over Wi-Fi Networks

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 devices with access to ePHI 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 tools 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.

Delete All Stored Health Information Before Discarding or Reusing the Mobile Device

When devices are outdated or no longer in use, it is essential to wipe all sensitive data before discarding the device. With AirWatch, this can be performed on facility-owned device remotely from the web-based console via a full device wipe. A device wipe removes all data from the device and restores it to its factory reset settings. Once a device no longer houses any patient data or organizational content, it can be safely recycled or discarded.

Ensure and Maintain Compliance of End Users

When operating in highly regulated industries, organizations must maintain compliance of all devices in a deployment. This can be a difficult task without a mobile device management solution in place. Through the AirWatch console, administrators have a comprehensive view of all devices that are enrolled into AirWatch Mobile Device Management. This enables administrators to oversee and analyze the device deployment as a whole and also gain insights into the compliance status of each individual device.
With AirWatch, organizations have the ability to tap into data driven solely by the users on their mobile devices. The console’s dashboard provides a snapshot view of a deployment at any point in time. The dashboard shows details at a glance, such as OS version and device model ratios, breakdowns of device ownership and devices out of compliance. Administrators can also run custom reports with in-depth content and application use information, enrollment status, compliance details and more.

AirWatch enables organizations to understand how users are leveraging devices, content and applications, which can help identify weak points in mobile security and ensure users are making the most of the secure access AirWatch provides.
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.