AirWatch - Security Considerations

Device Security Settings Changes / Passcode
Certain of your device settings will be required to change for AirWatch use. HIPAA and UMHS Compliance require that all devices that receive UMHS email or other UMHS resources be protected by a passcode with specific requirements. Those passcode settings and security policy restrictions include the following:

- A 6-character passcode is required (all numbers or alphanumeric). The passcode encrypts your device, and encryption is required for data and devices.
- With encryption, data can only accessed with your passcode.
- Device screenshots are disabled ONLY for devices that wish to access the MiChart mobile applications (Haiku/Canto). They are not disabled if you are only using/accessing UMHS Outlook Exchange email.
- Passcode history = 13 times (each time you set a passcode, it remembers the previous thirteen entries and will require a new, unique value).
- Passcode age = 365 days (after 365 days, you will be required to set a new passcode).
- Number of failed login attempts prior to device wipe = 10.
- Auto lock = at least 5 minutes (user can select a more secure value).
- Grace period before lock = at least 5 minutes (user can select a more secure value).

Level 2 Password Changes
Changing your Level-2 password on your workstation will not automatically change the password for Outlook Exchange email that you access on your mobile device through AirWatch. You need to reset the passwords independently. The recommended steps are:

- Put your mobile device in Airplane mode.
- Change your Level-2 password on your workstation according to the guidelines on the Change Password page.
- Take your mobile device out of Airplane mode.
- Access your email; you will receive a prompt to reset your password to the new Level-2 password you've chosen.
- Enter your new Level-2 password.

Lost or Stolen Devices
If your smartphone, tablet, or laptop is lost or stolen, and it contains UMHS data or applications (e.g. Outlook/Exchange email or MiChart), please contact the UMHS Service Desk immediately at 734-936-8000 so that they can assist you with locking or wiping the device as needed.

Wiping is a means to clear off data on a device. AirWatch keeps health system data and personal data separate which gives you the option of wiping either one or both. As a result, there are two types of "wipes" that AirWatch can do:

- Enterprise Wipe: Removes all data that was put on there by AirWatch, for example, UMHS Outlook Exchange email or any enterprise applications.
- Device Wipe: Removes ALL data on the device and returns it to factory defaults.

NOTE: Removal/wiping of personal or work data will not occur without your permission and identity verification.
Any replacement device should be enrolled using the instructions on the Enrolling in AirWatch page. You should not enroll a replacement device through the self-service portal.

Refer to Stolen or Lost Devices FAQs for more information.