AirWatch - Device Monitoring

For security purposes, AirWatch will only monitor activity as follows:

- If the device experiences "jailbreaking" or "rooting," all UMHS resources (including email) will be blocked until the approved operating system (OS) is reloaded. Jailbreaking (iOS) or rooting (Android) is the process of removing limitations on a device permitting direct access to the OS or installing a non-standard OS on the device.
- If the passcode or encryption is disabled, all UMHS resources (including email) will be blocked until the security options are re-enabled.
- If you travel outside the continental United States and your data plan does not cover international travel, your department can notify the carrier (AT&T, Sprint, or Verizon) to adjust the plan to reduce overage costs.

By policy, UMHS will not be monitoring any activity for personally owned devices, except for the following:

- If the device is compromised or rooted (see above definition).
- If the installation status of managed applications changes. Managed applications are the applications that UMHS makes available to its workforce. This does NOT include applications that the user downloads from iTunes, App Store, Google Play, etc.
- If the installation status of specific configuration policies is altered.
- Device metrics such as the phone’s serial number (in the case of theft or loss) - and then only at the specific request of and confirmation by the user.

Data Collection: AirWatch does NOT collect any data related to phone calls, texts, location, or web browsing. These capabilities have been disabled. AirWatch will not have any impact on your personal data. It provides the option of wiping UMHS data from the device since all personal and business-related data are kept separate.

GPS Tracking: Although GPS tracking is available via AirWatch, UMHS cannot actively monitor the location of mobile devices. Only the user may enable GPS if so desired.

Camera and Video Control: AirWatch cannot activate your device’s camera/video recorder, but it can push policies to the device to disable the camera if use or business cases warrant such restrictions.