

# Mobile Iron – Requirements and Questions

**Mobile Iron is a security application utilized by Methodist Le Bonheur Healthcare (MLH) to ensure network compliance of connected mobile devices.**

## Bring Your Own Device (BYOD) Requirements

---

### Operating System

**iOS** – iOS 8.0 or later

**Android** – Lollipop, KitKat, Jelly Bean, Ice Cream Sandwich

### Device Configuration Requirements & Settings

#### **iOS**

Password – Mandatory

Minimum Password Length – 6 characters

Maximum Inactivity Timeout – 3 minutes

Maximum number of Failed Attempts – 10

(NOTE: Device encryption is built into iOS devices.)

#### **Android**

Password – Mandatory

Minimum Password Length – 6

Maximum Inactivity Timeout – 3 minutes

Maximum # of Failed Attempts – 10

Device & SD Encryption

## Frequently Asked Questions

---

- 1. What is MobileIron?** Software used by MLH to secure and manage business applications, documents, and other business content on mobile devices and tablets. The MobileIron app provides IT with information about the device and its security state. This includes things like carrier, country, device make and model, operating system (OS) version, phone number, and corporate email.
- 2. How does it work?** IT uses MobileIron to set policies on mobile devices. For example, IT may set a policy that blocks a jailbroken device from getting company email. When the MobileIron app is installed on your device, you can:
  - Access your corporate email, calendar, and contacts (additional access form required)
  - Connect to “**DocNet**” – a private, Physician only Wi-Fi network

- Install Clinical Applications
  - Check compliance with MLH Security Policies
  - Locate lost or stolen devices
3. **Why does MLH want me to install MobileIron on my phone/tablet?** MLH uses MobileIron to protect patient information from being stolen or lost. Data theft can happen in many ways, but some examples include:
- Use of a jailbroken or rooted device
  - Running an older version of the operating system that has known security vulnerabilities
  - Installation of a malicious app that can steal information from other apps on the device
  - Connecting to the corporate network via an unsecure network - like the Wi-Fi in a coffee shop
4. **Can MLH read my personal emails?** No. MLH cannot read emails sent or received from personal accounts such as Gmail. If you are sending personal emails using your MLH account, MLH has access to that information, - the same way they do if you are using a PC/laptop. However, they cannot read or see your emails using the MobileIron console.
5. **Can MLH view my text messages?** No. MLH cannot view iMessages or SMS content.
6. **Can MLH access my personal contacts?** No. Only contacts associated with your MLH account will be visible to MLH.
7. **Can MLH access my photos/videos?** No. Photos and videos stored on your device are not accessible by MLH.
8. **Can MLH see what apps I have installed?** No. MLH can only see the apps we deploy.
9. **Can MLH access my voicemails?** No. MLH cannot monitor voicemail communications.
10. **Can MLH erase my device?** If your device is lost, **both you and MLH** can erase the device in order to protect your data.
11. **Can MLH clear my device passcode?** If you forget your device passcode, **both you and MLH** can clear it.
12. **Can MLH lock my device?** If your device is lost, **both you and MLH** can lock it with its passcode and specify contact information to retrieve the device.
13. **What can MLH do to my mobile device?**

- Block access to corporate email and internal resources if the device is out of compliance with company policies
- Require that certain apps be installed
- Lock or unlock the device **with your permission**
- Locate your device (**only if you chose to enable location services**)
- Wipe enterprise content off of your phone, leaving your personal information untouched **with your permission**


14. **What happens if I remove MobileIron from my device?** Your device will be out of compliance. Additionally, you may lose access on your mobile device to all MLH-related apps and data - including your MLH email, contacts, and calendar.

### How to Access the Above Information

---


#### iOS Device:

**Once MobileIron is installed, the information above is available by navigating to the following from your device:**

1. Go to the MobileIron icon 
2. Click Settings in the lower right corner
3. Click *Your Privacy*
  - a. To view what content remains private, click "*Personal content remains private*"
  - b. To view what MLH may access, click "*What's accessible by my company?*"
  - c. To view what MLH can control on your device, click "*What actions can my company take?*"
4. To view the MobileIron Privacy Statement go to *Settings > Your Privacy >* and choose *MobileIron Privacy Statement* at the bottom

#### Android Device:

**Once MobileIron is installed on a device the information above is readily available by navigating to the following from your device.**

1. Go to the Mobile@Work icon 
2. Click on the 3 lines in the upper left corner
3. Click *Settings*
4. Click *Your Privacy*
  - a. To view what content remains private, click on "*Secure Mobility*"
  - b. To view what information MLH may access, click "*Device Details*"
  - c. To view what MLH can control on your device with your approval, click on "*Remote Security*"
- 5) To view the MobileIron Privacy Statement click on "*View the MobileIron Privacy Statement*" under *Your Privacy*