MobileIron: What Partners Can and Cannot See on Your Device

Introduction

MobileIron is software used by Partners HealthCare to manage and secure mobile devices. As part of the process to register your device with Partners and to receive access to corporate resources like Partners email and Partners apps, you will need to install the MobileIron app on each personal device that you plan to use for business purposes. MobileIron tracks device information, such as the version of the operating system (OS) on your device, in order for Partners to maintain compliance with Partners policies. MobileIron also provides a way for Partners to wipe the device clean of all company information when a user leaves the company, or if the device is lost or stolen. It also monitors required security measures, like password length and complexity, to maintain compliance with Partners policies.

MobileIron: What Partners can and cannot see on your Device

The MobileIron Administrator can view non-personal device information (e.g. carrier and country, IMEI, MAC Address, etc.), and phone number (if applicable).

Partners cannot view personal email, photos, videos, phone activity (e.g. numbers called, duration, etc.), or web browsing activity on your device.

Feature/Functionality	Corporate Purchased	Personal Device BYOD	Notes
Corporate email	✅	✅	Only Partners Email Admins have this ability
Personal email Texts iMessages Photos Videos Voicemail Phone Activity Web Browsing Activity	🚫	🚫	Partners does not have access to **any** of this information
View **PHS** Apps on the device	✅	✅	Apps downloaded via the PHS "App Catalog"
View **All** Apps on the device	✅	🚫	
Location	✅	🚫	
User Name	✅	✅	Enrolled owner of the device
User Email Address	✅	✅	From Partners Active Directory
Phone Number Device Type and Model OS and Version Operator / Carrier Date / Time Registered IMEI Serial Number Wi-Fi MAC Address Used / Available RAM Used / Available storage Exchange ActiveSync Identifier	✅	✅	This information is automatically supplied by your device to MobileIron and is not configurable
Device ID	✅	✅	Android only

MobileIron: What Partners Can and Cannot See on Your Device

1. **Personally owned** iOS and Android devices, the MobileIron Administrator can only view business-related apps that are available in the Partners App Catalog. The Administrator cannot view any personal apps that you have installed on your device.

2. **Partners corporate purchased** iOS and Android devices, the Administrator can view all apps that are installed on the device. It is important for the MobileIron software to identify the apps that you have on your device in order to enforce company policy, such as requiring the MobileIron Go app or disallowing or "blacklisting" apps that could put the company at risk (e.g. from data loss or malware infection).

3. The MobileIron Administrator **cannot** view the location of your personally owned iOS or Android device.

4. The MobileIron Administrator **can** locate your Corporate Owned device using the MobileIron system if:

    a. You report it lost or stolen

    b. You have enabled the MobileIron app to access location services

    c. Location services are enabled on the device

What the Warning Means when You Register your iOS device with MobileIron

When you register your iOS device with MobileIron, you will receive the following warning prompt:

"Installing this profile will allow the administrator to remotely manage your device. The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your device."

This is a standard warning provided by Apple and the text cannot be changed to reflect what Partners has configured in the system. Please refer to the section above for a description of what the MobileIron Administrator can view on your device.

Why Does the MobileIron App Request Permissions when Registering Android Devices

When you register your Android device with MobileIron, you may receive the following warning prompt:

"*Allow MobileIron Go to make and manage phone calls?"*

PHS and MobileIron will **not** use this permission to make or manage calls nor does **not** provide PHS the ability monitor or track phone use. This warning is a standard warning by Google. Please refer to the section above for a description of what the MobileIron Administrator can view on your device.

When you register your Android device with MobileIron, you will be prompted to grant the app certain permissions. Android app permissions are static and defined in the app itself. They cannot be changed dynamically based on a specific company's configuration. This means that MobileIron apps ask for all of the permissions necessary to provide full MobileIron functionality even if the company will not be using those permissions. The table outlines the requested permissions and what they can be used for. Please refer to the section above for a description of what the MobileIron Administrator can view on your device.