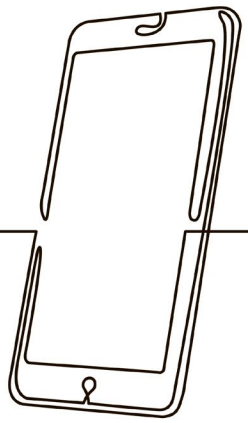
MobileIron

Frequently Asked Questions



About MobileIron

MobileIron is a mobile device management (MDM) system that provides ITS with a means of governing mobile access to WCM resources, including email, calendar, contacts, and other central applications. Through the use of MobileIron, which is a free application that is installed on a governed mobile device, ITS has the ability to configure devices with the appropriate WCM settings to allow access to Wi-Fi networks, a WCM email account, and WCM applications. As a benefit to both WCM and the end user, MobileIron helps manage compliance with security policies and other regulations by enforcing device encryption and the use of a passcode to reduce the risk of accidental or improper disclosure of data in the event the device is lost or stolen.

Is MobileIron required for my device?

Yes. Any mobile device (smartphone or tablet) configured with a WCM email account (or wishing to access the WCMC Wi-Fi network) must have MobileIron installed. Without MobileIron, WCM cannot ensure the security of all devices with WCM data. In the event the device is lost or stolen, there are no assurances that WCM data has not been breached or inappropriately disclosed. Weill Cornell Medicine's faculty, students, and staff create and share a wealth of information on their mobile devices every day, much of which may be confidential or high risk. Should your device become lost or stolen, ITS can attempt to locate and wipe your device remotely at your request to help make sure this data never gets into the wrong hands. Even if you do not regularly work with high risk data, it can protect the other content on your phone and is necessary for inventory tracking by your department. Not only does it protect you, it protects everyone who does business with Weill Cornell Medicine.

I don't access clinical or high risk data. Do I still need MobileIron?

Yes. WCM's definition of high risk data extends beyond protected health information (see ITS policy 11.03 - Data Classification). If you use your mobile device to access the WCMC wireless network, you are using Weill Cornell Medicine resources and will need to have MobileIron installed.

MobileIron Privacy

Can ITS spy on my mobile device once MobileIron is installed?

No, ITS cannot spy on your device through MobileIron, nor is ITS interested in actively monitoring your device. In addition, ITS enforces very minimal requirements and restrictions on your device – a password, which enables encryption. Here are things MobileIron does not do:

- View or read your messages
- View your pictures or other multi-media
- View your website browsing history
- Turn on your camera to take photo or video
- Listen in on your conversations
- Open or delete your files and applications
- View contents within your applications
- Drain your battery

Also, ITS does not read individual emails in your Weill Cornell Medicine account, nor can we access any personal email from external sites like Gmail or Yahoo! Mail. ITS uses a data loss prevention software in accordance with College policy (see 11.02 - Privacy of the Network and 11.09 - Data Loss Prevention) to make sure confidential data is not sent to external accounts (those that do not end in @med.cornell.edu) without encryption.

It is important to note that although ITS does not actively monitor emails, Weill Cornell Medicine reserves the right to access, review, and release electronic information under circumstances necessitated by legal or regulatory requirements.

What information does MobileIron collect about me and my device?

MobileIron collects the following information about your device:

- Identifying information about you, the end user, so ITS is aware who the device belongs to. This includes your name and your WCM email address.
- Device specifications, including the make and model of the device you are using, the device's phone number (if necessary), the device's operating system and version, your cellular/data provider, the device serial number, status of the battery percentage, etc.
- Amount of used and available space on your device.
- A list of applications on your device to ensure the MobileIron and WCM-deployed applications are installed and kept up-to-date.
- Location data, if you grant permission to the MobileIron application, in the event your device is lost or stolen and you request ITS to help you locate it. Please note that ITS does not use this data to actively monitor your location and it will only be viewed at your request.
- Status of the MobileIron application, the security certificate, and security status.
- An inventory of installed security certificates, security compliance profiles (e.g., password settings), a log of Mobile Device Management (MDM) communications (e.g., last check-in time with the server, diagnostic errors).