

Frequently Asked Questions & Answers:
Bring Your Own Device (BYOD) Policy

Converting a Device

- **Whose phones will be wiped on Wednesday, January 30?**

If you continue to have a company-paid phone, you are at no risk of having your device being wiped on 1/30/2013. The only phones that are at risk of being wiped are the formerly Kindred-owned/RehabCare-owned phones that meet one of the following conditions:

1. If it wasn't moved to a personal-liable account but should have been moved to one.
2. The phone has been moved to a personal-liable account and it isn't setup with the Mobile Iron application on the MI3.kindredhealthcare.com server.

If you need assistance moving your phone to a personal-liable account or installing email on it, please contact Kindred Mobility Support (Mobi) at 866-810-9769.

- **What is MobileIron?**

MobileIron is software used by Kindred to manage and secure mobile devices. As part of the process to register your device, you will 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 the company to maintain compliance with the Mobile Device Policy. MobileIron also provides a way for Kindred to selectively wipe the device clean of all company information without removing personal information or files should you leave the company, switch devices, or your device is lost or stolen. It also monitors required security measures, like password length and complexity, to maintain compliance with the Mobile Device Policy.

- **When the MobileIron app is on my device, what can the Administrator see? Can they see my photos, files, texts, etc.?**

The MobileIron Administrator can view non-personal device information (e.g. carrier and country, IMEI, MAC Address, etc.), phone number (if applicable), the apps that are installed on your device, and the device's location. MobileIron does not provide Kindred any access to personal files on your device or web site history or shortcuts. Files include photos, text messages, email, notes, address lists, etc.

- **What happens if I remove the MobileIron app from my device?**

If you remove the MobileIron app from your device you will not be able to access corporate email, contacts and calendar on the device until you reinstall the MobileIron app.

- **Will I have to use a passcode with my personal device?**
 Yes. If you want to access corporate email on your personal device, Kindred will enable the corporate password policy on it, which means you must enter the device's passcode every time you use the device.
- **My device is not eligible for the BYOD. Are there plans to add to the list?**
 At this time, only iOS and Android devices are registered with MobileIron. Other mobile operating systems, such as Windows Phone 8, will be evaluated as the program evolves. Blackberry devices utilize the same infrastructure as Corporate owned devices and do not need to be re-registered. However, Blackberry users will need to contact MOBI if they move their corporate phone to a personal plan and want Kindred email on it.
- **Can I register both my personal smartphone and tablet?**
 Yes, you may register both and receive email, calendar, and contacts on both.
- **Can I register my personal device if it is rooted or Jail-broken?**
 No. Rooting your Android, or Jail-breaking your Apple device potentially disables the data security features that are required by Kindred Policy. If you register a rooted or Jail-broken device through the BYOD portal, a single email will be sent to you and your supervisor via the Kindred email of record stating that the device is compromised and cannot contain Kindred data. A selective wipe, removing Kindred data, will be issued to the device. If the device is re-registered without being "un-rooted", it will receive a full wipe, (reset to factory defaults) and access to email via remote devices will be disabled.
- **What is TouchDown and why do I need it? (Android Only)**
 NitroDesk's TouchDown app is an encrypted email and calendar client for Android devices. The native email and calendar clients on most Android devices do not support key business requirements, like encrypted email. TouchDown provides secure corporate email and calendar access on your personal device.
- **How do I install TouchDown on my Android device?**
 TouchDown is available from Google Play (formerly Android Market). Please follow the instructions for installing and configuring TouchDown in the registration instructions provided.
- **When I install "Touchdown", I installed the free version. The free version is a 30-day trial. The complete version costs \$19.99. Will the company be reimbursing people for the Touchdown license? Do you or IT know if we can use the free version indefinitely though it says it is a 30-day trial? Some Android applications will allow you use the free version indefinitely but with limited functionalities?**
 You should always select the free version and you don't have to worry about the 30-day expiration. After you connect to the Kindred environment, we will apply the required license information at no cost to the employee.

Privacy

- **I have an Apple device. On page 8 of the email install for Apple PDF there is a certificate that says that Kindred has the right to have access to and manage personal data on the phone. Am I misunderstanding this? What exactly does this mean?**

The certificate refers to the functionality of MobileIron. In order to manage Kindred email on your device, we can see your security settings, phone serial number, jail broken status and the list of applications on your phone. We cannot see any of your personal files or data for your applications. This means we cannot see your pictures, music, files, personal contacts, notes in your notepad, etc. In addition, we cannot read your personal emails or any text messages you send. These communications do not go to any Kindred server and the software you use to access your Kindred email and calendar cannot access any other phone applications or data.

- **I don't typically mix business and personal on any of my phones, computers, iPad for what I think are obvious reasons. What protection do I have now that my personal phone appears to be becoming a company device? Does my privacy have any protection in the case of a breach?**

Your personal phone will always be your personal phone. We cannot see any file data or email data on the device. The MobileIron application needed to access Kindred email on a personal device does not provide Kindred (or anyone who might break into Kindred's systems) any access to personal files on your device or web site history or shortcuts. Files include photos, text messages, email, notes, address lists, etc.

- **Can you tell where I am if I install MobileIron?**

Yes. Kindred will be able to determine where your phone is if you have enabled MobileIron to access location services and if you have enabled location services on the device to remotely locate the device. If you disable location services for MobileIron on your device then Kindred cannot locate the device. Note, you will be able to access Kindred email, calendar, contacts, etc. regardless of the location services setting value.

Kindred Support

- **What company resources are available from my personal device?**

Corporate email, calendar, and contacts, are supported on personal phones at this time. Additional Kindred applications may be supported on phones or tablets in the future.

- **The End-User License agreement says that users may only put "Certified Applications" on their mobile device. What applications are supported? Are there any apps that are not allowed?**

This requirement applies to company-owned phones only. At this time, Kindred is not restricting the use of mobile apps on your personal device. This policy may be revised in the future to discourage installation of apps that may put the company's corporate data at risk.

- **If a personal device is lost or stolen, is there a way to remotely get the location of the device?**

Yes. If your device is lost or stolen, report it to the Kindred Compliance hotline. Kindred Technical services can locate your device if you have location services enabled for MobileIron. However, for safety reasons, Technical services will not provide you with the location of your device, particularly if it's reported lost or stolen. If requested by the Kindred compliance department, Technical services will provide location information to the compliance department in order to provide it to local law enforcement.

Returning Device to Factory Defaults

- **When a device is wiped back to factory defaults, is all content wiped including email, photos, and applications?**

Yes. By policy Kindred can reset your device to its original factory settings, which would erase all data on the device. In practice, a personal device will likely only be "wiped" or reset to factory defaults if it is reported to compliance as lost or stolen, or the security features are compromised, and Kindred data is at risk.

- **Can only corporate data on personal devices be wiped, leaving my personal data on the device?**

Yes, corporate data can be removed while preserving personal data. This is one of the benefits of installing MobileIron. This process is known as a selective wipe. For example, should you leave the company, the company will perform a selective wipe of your personal device to remove access to corporate resources, leaving your personal data, photos, etc. intact.

- **What happens to my data if I am separated from the company?**

All corporate data will be removed from the device via MobileIron as part of the off-boarding process. Personal data will not normally be affected but it is always good practice to backup your personal data in case you need to restore your files.

Stipend/Company-owned Phone

- **Does the \$35 stipend apply to phone, data/e-mail/texting use for Kindred business? Will we be able to receive some kind of message when we have hit our \$35?**

The \$35 monthly stipend will be included in your regular paycheck. It is yours to use however you see fit, however its intent was to help defray the costs of the monthly fees associated with a cell phone for use related to Kindred business. Any arrangements regarding messages as to the usage of your phone will have to be made with your individual carrier.

- **What if I don't agree to use the stipend and the company phone?**

You may opt to not use the company phone and may chose to add Kindred email and calendar to a personal device by installing the MobileIron application. The stipend is for you to use as you see fit. If you accept the stipend, you will be expected to put Kindred email on your device.

- **Who is eligible for a stipend or a company-funded phone?**
Individuals/titles with certain responsibilities that require a company-phone or support through a stipend were identified by job function and communicated with directly.
- **What is the process when devices that will be terminated in error and should be company liable or stipend? What is the turnaround time for the service to be up and running?**
If a company liable or stipend device is accidentally terminated, the user should call Kindred Mobility and indicate their device has been disconnected accidentally. Kindred Mobility will verify the user and title against the master list of titles to assure the device should be reactivated. They will send a verification request to Kindred's Voice Services team as well. Kindred Mobility will make every effort to re-instate the user's device while they are on the phone. If the user does not have one of the approved titles, Kindred Mobility will direct them to their management.