Student Mobile Device agreement

UW SMPH \ UW Health Mobile Device Terms of Use:

If your device is lost or stolen:

- Please immediately notify desktop.support@med.wisc.edu
- If your device is lost or stolen on the UW-Madison campus, report it to the UWPD at 608-264-2677.
- If it is lost or stolen elsewhere, report it to the appropriate local law enforcement agency.

When I connect my mobile device to the UW Madison Mobile Device Management System (Workspace ONE) used by SMPH, I understand that the following security requirements will be technologically imposed on my device:

- A code (PIN), phrase, screen swipe pattern, or similar user entered authentication mechanism will be imposed before the device can be used for access to applications or data on the phone. The mobile device owner will be solely responsible for remembering this access code.
- After a period of inactivity, the user will be required to re-enter the access code to access the device.
- If an incorrect access code is entered repeatedly, the device will be remotely erased.
- Data stored on the device will be encrypted.
- The mobile device owner is responsible for backing up all personal data (photos, music, documents, etc.) to a location off of the device. If the mobile device must be remotely erased, personal data on the device may be destroyed.
- The user is expected to immediately contact the SMPH Shared Services IT if the unit is lost or stolen. If reported lost or stolen, the device will be remotely erased the next time it connects to any data network to assure both patient and sensitive business data are not accessible to unauthorized persons.
- Upon termination of employment, all corporate data and software will be remotely deleted from the device. Personal data and software will not be deleted.
- UW Health IS will monitor connections from mobile devices to the MDM system. Users with registered mobile devices that have not connected to the MDM system in over a month may be disconnected from the MDM system.
- All devices enrolled will have a minimum OS requirement and are expected to be kept current.
- Corporate applications should be installed on the device only from the mechanisms provided by UW Health IS. Users should not install versions of the same software from publicly available application sources (i.e. “app stores” like iTunes or Google Play/Android Market) unless directed by IS.
- Additional security mechanisms may be activated on the device to address potential vulnerabilities as they become known.

I further understand that additional security mechanisms, or changes to existing security mechanism, may be activated on my device to address potential vulnerabilities as they become known.

I understand that SMPH Shared Services IT reserves the right to monitor my use of corporate resources on my device, including e-mail and calendaring, with or without notice, and therefore I should have no expectations of privacy in the use of these resources. UW Health IS will NOT monitor use of non-corporate applications on my device.

* Note: Support for these mobile applications is provided via the SMPH Shared Service IT by email desktop.support@med.wisc.edu Monday-Friday from 8am–5pm only.

I agree that I will make no attempt to circumvent any security mechanisms placed on this mobile device and understand that violation of this requirement may result in suspension of mobile device privileges and/or disciplinary action up to and including termination of employment.