Mobile Device Access End User Agreement

I, the undersigned, understand that Boston Children’s Hospital (BCH) is allowing me to access information that I have been authorized to access as part of my job using either a personal or BCH owned mobile devices such as smartphones and tablets. I will allow BCH to take appropriate steps to ensure the safety and security of their data.

In order to comply with Federal and State regulations, management of mobile devices will require security configurations that include inactivity timeouts, PIN and/or passwords requirements, native encryption on the device, and remote wipe capabilities. BCH reserves the right to block access to its data when/if it is determined that the mobile device has been infected with known malicious software or the mobile device does not have the required security configurations active and current.

Removing, changing, or reducing the effectiveness of the required configured security settings is not allowed while the device is used to access BCH systems and data. Additionally, tampering or removing the phones built-in operating systems security controls is not allowed. Periodic upgrades may also be required to remediate announced security vulnerabilities.

Most smartphones and other mobile devices come with encryption preloaded on the device. On certain older phones, encryption may not be a standard installation on the phone. A user can only use a device that has native encryption. I understand that it is my responsibility to purchase mobile devices that come with encryption. BCH Information Security Department (BCH ISD) will be available for assistance in confirming native encryption is engaged on your mobile device at Fegan 190 (by the elevators). All laptops that access Boston Children’s systems and data must be encrypted. Laptops that are not encrypted cannot be used on the hospital network or for hospital business. If I have any questions I will call or email the Help Desk, and request help from a technician.

I am personally responsible for notifying the BCH ISD as soon as reasonably practicable when my mobile device is lost, stolen, replaced, sold, traded, given away, or out of my possession. I give BCH ISD permission to remotely wipe the device (i.e. full data wipe) to protect any sensitive data such as ePHI and/or PI that may have been accessed on the device. I will also allow BCH ISD to remotely wipe my mobile device, if I am voluntarily or involuntarily terminated from BCH. I understand that remote wiping a device will delete any photographs, music or other information stored on the device. It is strongly recommended that I back up any personal data on my device on a regular basis to an approved cloud provider. Backing up my personal data is the best way to ensure my personal data does not get lost or deleted due to a remote wipe of my device. BCH understands the sensitivity of a remote wipe. By providing advance notice, BCH may be able to work with the end user to minimize any risk of losing data.

I understand that I must fully comply with BCH Policies and Standards of Conduct and that saving and storage of ePHI and/or PI data on my mobile device is strictly prohibited.

I understand that a violation of the terms and conditions set out in the policy may result in the restriction and/or termination of my mobile device access to the BCH ISD network, and may result in further disciplinary action up to and including termination of employment and/or other legal action. I further understand that failure to comply with these policies could require BCH to file a report with federal or state authorities.

Print Name:

Signature:

Date:

Phone:

Email Address