Mobile Device Security Toolkit

Sample Mobile Device User Agreement

Introductory Note: *The sample mobile device user agreement is an example of an agreement that is being used by a health system to manage personal mobile devices in its environment. It is only an example and is not meant to be a complete or exhaustive list of policy elements. Because organizations, along with regulatory and legal requirements, are different, each organization should develop a unique mobile device user agreement that is aligned with the needs of the organization, applicable laws, and is consistent with its policies and procedures.* ***Nothing herein contains any legal advice or any other kind of advice whatsoever. This information is being provided for educational purposes only.***

As a condition of synchronizing my personal mobile device with the XYZ Health System computing environment, I release remote administration rights and understand that I am subject to certain restrictions and expectations on the use of my mobile device. This document serves as notification of the restrictions and expectations, and acceptance and acknowledgement thereof.

By signing below:

• I agree to follow all XYZ Health System policies relating to the use and security of portable computing devices.

• I acknowledge that XYZ Health System will enforce security settings on the mobile device including at a minimum encryption of all XYZ Health System information, and remote wipe capabilities where applicable on said device.

• I understand that if I do not make appropriate backups of my personal information maintained on the mobile device in order to avoid loss of information should the device be lost, stolen, corrupted, or data must be deleted (wiped) in order to protect sensitive information, such personal information may be lost and is not the responsibility of XYZ Health System.

• I agree not to backup XYZ Health System information (including e-mail) to a non-XYZ Health System computer or move the XYZ Health System information from its encrypted area to any other areas on the smart phone. I understand my XYZ Health System email mailbox information is maintained and backed up by XYZ Health System and should not be replicated onto non-XYZ Health System computers.

• I agree to hold XYZ Health System harmless for any loss relating to the administration of mobile device connectivity to XYZ Health System systems including, but not limited to, loss of personal information stored

on a mobile device due to data deletion done to protect sensitive information related to XYZ Health System, its patients, members or partners.

• I understand that modifying the underlying operating system of the device (e.g., “rooting”, “Jailbreak-ing”, etc.) will result in the device being removed from synchronization with XYZ Health System data and voids this agreement and support for the device.

• I understand and accept that synchronization relies on one or more cellular network providers and the Internet, and that both are subject to slowdowns and outages of extended duration that are beyond the control of IT. Service cannot be guaranteed or fixed by XYZ Health System.

• I understand that access to the XYZ Health System wireless network is not available to non-XYZ Health System devices. All connectivity must be through cellular provider.

• I agree not to transmit XYZ Health System sensitive information (e.g., Business Sensitive Information (BSI) or Protected Health Information (PHI)) through non-XYZ Health System approved methods. These include texting, paging, personal email and social networks. Electronic communications with patients should be through XYZ Health System. BSI can be transmitted using secure e-mail (e-secure) of secure file transfer methods.

• I understand that these devices should not be considered diagnostic quality for patient care decisions, and should not contain Protect Health Information (PHI), unless incorporated as part of an officially approved, standard application support by XYZ Health System.

• I agree that the mobile device can be wiped remotely by XYZ Health System upon the decision of XYZ Health System management and understand that it will delete all data including personal files.

• I agree to report loss of a device immediately to the IT Help Desk xxx-xxx-xxxx.

• I understand that non-exempt employees carrying or operating a mobile device outside of normal work hours does not constitute working remotely unless properly authorized by management.

• I understand that failure to adhere to these conditions or failure to appropriately safeguard XYZ Health System information could result in action against me personally, including termination of employment, civil action (e.g., being sued directly) or criminal prosecution by effected persons. [This exposure is especially relevant to disclosure of Protected Health Information (“PHI”) or Business Sensitive Information (“BSI”)].

Printed name: _____

Signature: _____ Date:_____

Manager Approval printed name: _____

Manager Approval Signature: _____ Date:_____

Accounting Unit: _____ Expense Code: _____

Department: _____