BRING YOUR OWN DEVICE (BYOD) POLICY

TABLE OF CONTENTS

Policy Overview

Bring Your Own Device (BYOD) refers to employees using personally-owned mobile devices (i.e. smartphones, tablets and wearables) to connect to hospital resources. *<The hospital>* allows BYOD, but requires that all employees acknowledge and comply with this written policy before using personally-owned devices to connect to hospital resources.

The purpose of this policy is to define eligibility for BYOD, associated financial responsibilities, the roles and responsibilities of the BYOD employee, security requirements for BYOD, IT support of BYOD and penalties associated with non-compliance. While *<the hospital's>* BYOD policy ensures reasonable protection of personal data, security of sensitive hospital data is the primary goal of the policy. Access to highly sensitive data, such as Protected Health Information (PHI), requires strict adherence to security standards, which are upheld by this policy to protect patient privacy and safety.

All employees who wish to use a personally-owned device for patient care related activities must opt-in to *<the hospital's>* BYOD program by signing off on this policy before using any personally-owned device to connect to hospital resources.[i] All employees who opt-in to *<the hospital's>* BYOD program are required to accept the terms and conditions for acceptable use of personally-owned devices outlined within this policy, including but not limited to: acceptance and acknowledgment of requirements related to data management and removal, password enforcement, data backups, device settings management, and data discoverability.[i]

SECTION 1: Eligibility

BYOD eligibility for all employees will be decided by department managers, based on the following guidelines and requirements:

a. The employee's status must be within scope of this policy (see section 1a).
b. The employee's personal device must be on the supported device list (see section 1c).
c. The employee's use of BYOD must reside within *<the hospital's>* supported BYOD models (see section 1d).
d. The employee must be employed full-time with responsibilities deemed appropriate for BYOD by the department manager.[i]
e. There must be a justifiable business need for the use of a personal device.
f. The employee does not work in what is considered to be a high-security area.[i]

1a) Scope

The scope of this policy covers all full-time employees who access *<hospital>* resources via personal devices. Hospital-owned devices are considered outside the scope of this policy, as they are covered by the hospital's smartphone security policy. Laptops and personal computers are not considered a part of this policy, as they are covered by a separate policy. Part-time and affiliate employees are also considered outside the scope of this policy, as they are not eligible for BYOD.

1b) Applicability

Device use case that are covered by this policy include:

a. Devices that are used to access hospital-owned data via mobile applications or websites (i.e. EMR applications, etc.).
b. Devices (smartphones, tablets and wearables) that are used to send, receive or store hospital email or other hospital-owned data.
c. Devices that are used to send or receive sensitive data via text, images or video.

1c) Supported devices

The following platforms, devices, operating systems, and applications are supported for BYOD (note: supported platforms, device models, operating systems or applications are subject tot change anytime without notice to the employee):

Platform	Device Models	Operating Systems	Applications
Amazon Kindle	Not Supported	N/A	N/A
Android	*<Samsung Galaxy S3, Motorola Moto G, Samsung Galaxy Note2-4, Samsung Galaxy S4, Samsung Galaxy Grand Prime, Samsung Galaxy Tab3, Samsung Galaxy S5, Samsung Galaxy S3 Mini, HTC Pne M8, HTC One Mini 2, Nexus 5, Nexus 6, Sony Xperia Z3*	*<greater than or equal to KitKat 4.4>*	*<Spok Mobile (Secure Text Messaging) Epic Haiku (EMR)>*

Apple	*<iPhone 4, iPhone 4S, iPhone 5, iPhone 5C, iPhone 5S, iPhone 6, iPhone 6S, iPad 2, iPad Pro, iPod Touch 4G, iPod Touch 5G, iPod Touch 6G>*	*<greater than or equal toiOS 6>*	*<Spok Mobile (Secure Text Messaging) Epic Haiku (EMR) Epic Canto (EMR)>*
RIM (Blackberry)	*<Not Supported>*	*<N/A>*	*<N/A>*
Windows	*<Not Supported>*	*<N/A>*	*<N/A>*

Note: Some departments may have specific requirements for mobile devices, such as sleds or peripherals. If these are not compatible with BYOD devices, it will be the department's responsibility to provide a hospital-issued device and/or discuss alternative options with the employee.

1d) Supported BYOD models

<The hospital> supports the following BYOD models:[i]

a. Employees who are not eligible for a hospital-owned device can use a personally-owned device to access hospital resources, as long as they meet the requirements for BYOD outlined within this policy.
b. Users who are eligible for a hospital-owned device can choose to opt in to BYOD instead and use a personally-owned device to access hospital resources, as long as they meet the requirements for BYOD outlined within this policy.
    - Note: Opting in to BYOD makes the employee no longer eligible for a hospital-owned device - if a hospital-owned device has already been provided to the employee, that device must be relinquished upon opting in to BYOD.

SECTION 2: Expense Allocations

Upon opting in to *<the hospital's>* BYOD program, employees must accept responsibility for all costs associated with procuring devices, replacements for lost, damaged or stolen devices, device accessories, and mobile provider services (voice, text and data plans). *<The hospital>* will not assume responsibility for any costs associated with the use of personally-owned devices.*

*Exceptions outlined in section 2a.

2a) Stipends and discounts

The following stipends and discounts are offered to assist employees with costs related BYOD:

a. **Stipends**: If the use of a personally-owned device is deemed as essential to job function, as decided by the department manager, a monthly *<$ amount>* stipend can be supplied for assistance with mobile provider services. This stipend is to be added to the employee's paycheck on a monthly basis. Stipends are not available without manager approval and formal request to hospital administration that the use of a personally-owned device is essential to job function.
b. **Discounts**: *<The hospital>* has a preferred vendor agreement with *<vendor>*. Per this agreement, all employees are eligible for a *<% discount>* on all subscriptions, plans and accessories from Verizon Wireless. To receive the discount, all devices, subscriptions, plans and accessories must be purchased directly from the preferred vendor and a hospital ID must be presented upon purchase.[i]

SECTION 3: User Roles and Responsibilities

All employees must comply with this policy by understanding and assuming appropriate ownership of these roles and responsibilities.

3a) Acceptable use

Given that all guidelines and conditions outlined within this policy are met, the following use cases are permitted and acceptable use of personally owned devices:

a. Messaging of hospital related content between care providers over known secure networks, using the hospital's supported secure text messaging application.
b. Receiving alarms from clinical systems nurse call, patient monitoring, lab results, etc.) over known secure networks, using the hospital's supported secure text messaging application.
c. Accessing PHI over known secure networks, using the hospital's supported EHR application.
d. Using third party applications, such as drug reference guides and medical calculators, to access clinical data that is not owned by *<the hospital>.*
e. Accessing hospital email over known secure networks.

The following use cases are not supported, allowed or permitted:

a. Messaging of hospital related content between care providers using using standard text messaging (SMS) or any third-party consumer messaging application (i.e. WhatsApp, WeChat, etc.).
b. Accessing personal apps, email or websites while on clinical duty.
c. Use of unsecure third party applications to view or transmit sensitive data, such as PHI.
d. Using the device for any reason while driving.
e. Download or use of any applications that are blacklisted, or deemed inappropriate by the hospital or by department managers.
f. Sending highly sensitive data, such as PHI, over non-secure public Wi-Fi networks.

3b) On call policies

The following responsibilities are applicable to any employee that is on call for a clinical service, regardless of specialty.

On call physicians and staff must *always*:

a. Remain available while on call.
b. Keep the device closely accessible, charged and powered on while on call.
c. Contact the department and receive prior approval for any scheduling changes.

On call physicians and staff must *never*:

a. Remove secure text messaging software from their device at any time.
b. Use device Do Not Disturb while on call.
c. Change their secure text messaging status to not available while on call.

3c) Device maintenance

Employees are responsible for keeping their devices in working and compliant condition at all times. This includes the following responsibilities:

a. Manage power to ensure that mobile device batteries remain charged throughout the entire shift and the device stays powered on.
b. Ensure that the device is supported (on the supported device list in section 1c).

c. Ensure that device settings and configuration are within compliance of this policy. [i]
d. Ensuring that the device is kept clean and protected against cross-contamination, within patient health/safety standards.

3d) Loss/theft

<The hospital> will not be held liable for lost or stolen devices. Employees are responsible for the following:

a. Take reasonable precautions to prevent loss or theft of the device.
b. Do not sell or discard the device without first notifying hospital IT, via the helpdesk.
c. Report lost or stolen devices within 24 hours of learning of loss/theft.[i]

Note: Hospital IT will issue a remote wipe of all hospital data from any lost or stolen devices. This may include removal of any personal data on the device. It is the user's responsibility for backing up all personal data to prevent any loss of that data.[i]

3e) Warranty and replacement

<The hospital> will not be held responsible for replacing lost, damaged or stolen devices under any circumstance. Employees will not be reimbursed for lost, stolen or damaged devices. The hospital will not assume responsibility for acquisition of replacement devices. It is the responsibility of the user to work with the mobile provider, device manufacturer or other third-party to obtain a replacement device in the event of damage, theft or lost.[i]

Note: The help desk will provide temporary loaner/spare pagers for patient critical personnel and on call physicians and staff while device replacements are obtained.

3f) Application downloads and upgrades

Employees are responsible for ensuring that all applications and content on devices used to connect to hospital resources are trusted, appropriate and kept up-to-date. Employee responsibilities include:

a. Only download applications from trusted public app stores or hospital-owned locations. Never download untrusted applications that have been blacklisted by the hospital.[i]
b. Ensure the latest version of the software for all applications that are used to connect to

hospital resources.

c. Maintain an Apple/Google ID and password containing valid identity information.
d. Do not expense applications, unless approved by a department manager.[i]
e. Research applications and take reasonable precautions to avoid downloading malicious software.
f. Comply with required hospital application updates within 48 hours.
g. Do not attempt to jailbreak/root a device.

3g) Transmission and storage of highly sensitive data

Sensitive data, such as Protect Health Information (PHI), Personal Identification Information (PII), and financial information is subject to all requirements outlined within this policy, as well as, additional security measures:

a. Employees must never use consumer text messaging (SMS) or third-party messaging applications to transmit or store PHI or other highly sensitive data.
b. *<The hospital's>* approved secure text messaging application is required for transmission and storage of all highly sensitive data. This included data in text messages, pictures and videos.
    - Note: Orders should not be sent via the hospitals secure text messaging application.
c. Employees must acknowledge that all messages sent via *<the hospital's>* secure text messaging application are subject to audit and/or remote message removal.
d. Employees are never permitted to store highly sensitive data on local device storage, including storage of text, pictures, video or other files.
e. Employees are prohibited from taking screen shots of sensitive information that is stored within trusted, secure hospital applications, such as secure text messaging.
f. Employees are responsible for ensuring a secure environment, including:
    - Employees are required to keep all passwords/codes private and protected.
    - Employees must not provide passwords/codes to any other person.
    - Employees must not leave mobile devices unattended to be viewable and accessible by unauthorized individuals. Mobile devices must be locked before leaving them unattended.

3h) Backup and file sharing

Employees are responsible for ensuring that all data on the device is properly backed up.

a. All hospital-owned and/or sensitive data must be backed up and synced to approved locations

only. Hospital IT generally ensures hospital-owned data is backed up, but it is the employee's responsibility to ensure that data is not copied or backed up to unsecure locations, such as public cloud storage.

b. Consumer backup software, public clouds and personal email are prohibited from use for transfer, sync or storage of hospital-owned and/or sensitive data.[i]

c. Employees are responsible for backing up all personal data (personal pictures, videos, files, etc.) to preferred sources.[i]
    - *Note: <The hospital>* will not be held liable for any content that is permanently lost in the event that the device must be remotely wiped and the employee has not backed up personal content.

3i) Termination of employment

<The hospital> will wipe all devices that contain hospital data upon termination of employment. In most cases, personal data will not be wiped from the device (only hospital data will be wiped); however, in some cases the entire device will be wiped. It is the employee's responsibility to backup personal data within the guidelines of this policy (see section 3h) to prevent personal data loss.

Any attempt to restore hospital data subsequent to termination is considered highly prohibited and subject to legal action.[i]

SECTION 4: Security and Feature Management

<The hospital> will enforce security standards to ensure adherence to regulatory and compliance guidelines. These guidelines include HIPAA technical safeguards (see appendix A). The primary objective of these security measures is to protect the patient's right to privacy, in accordance with government and regulatory requirements. The objective is not to impede on an employee's privacy; however, all employees who opt in to BYOD must comply with all security requirements to ensure protection of sensitive hospital and patient data, which may require the employee waive the right to privacy. All hospital data that is stored on a device must be secured using hospital-mandated methods at all times and all employees must abide by hospital security policies.

4a) Device/feature management

a. *<The hospital>* will install Mobile Device Management (MDM) software on all devices that are used to access hospital information. This software will be used to restrict features and settings that may introduce security vulnerabilities. The employee must never remove this software

unless all access to hospital data is removed prior to removing the MDM profile.

b. Jailbreaking/Rooting is not allowed on any device that is used to access hospital resources. Any device that is not compliant with this rules, will be subject to the penalties outlined within section 6 of this policy.

c. *<The hospital>* will enforce passcode requirements on any device used to access hospital resources.
    - The password policy for mobile devices requires a minimum of six digits (numeric), must be updated every ninety days, must timeout after five minutes, and must be unique for six password changes.

d. Security safeguard, such as encryption and settings management, will be applied when accessing hospital applications and data.

e. Mobile device cameras are not permitted in patient areas and may be disabled by MDM software.

4b) Transmission and storage of highly sensitive data

a. *<The hospital>* will install a secure text messaging application on all devices that are used to transmit highly sensitive data. *<The hospital>* may also ask the employee to install the secure text messaging application.

f. The secure text messaging application will provide encryption, access codes, automatic message removal, auditing and access control capabilities to protect sensitive data.

g. *<The hospital>* will install an application for accessing Electronic Medical Records (EMR) on all devices that are used to access highly sensitive data. *<The hospital>* may also ask the employee to install the EMR application.

h. No other application is to be used to store or transmit or store highly sensitive data.

i. *<The hospital>* will manage all backups of highly sensitive data. The employee will not be permitted to backup highly sensitive data.

4c) eDiscovery

In the event of legal, government or regulatory requirement, *<the hospital>* may be required to produce data from any device that is used to transmit or store hospital data. If this occurs, hospital IT may notify the employee that data will be required from the device and a remote data audit will be conducted. In the event that hospital IT cannot access the data remotely, the employee must physically supply the device to IT, along with all content and passcodes.[i]

Note: In most cases IT will be able to separate hospital data from personal data, but in some cases

the device's entire contents may need to be discoverable.

4d) HIPAA technical safeguards

The requirements below will be strictly enforced on any device that is used to access highly sensitive data, such as PHI, based on HIPAA technical safeguards (see appendix A).

a. Settings will be applied to require automatic logoff of the device. This will require employees to sign back in after a period of inactivity on the device.
    - HIPAA Technical Safeguard: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.[ii]

b. Encryption will be enforced on all devices by MDM software.
    - HIPAA Technical Safeguard: Implement a mechanism to encrypt and decrypt electronic protected health information.[ii]

c. Data from the device will be collected and logged for compliance reporting purposes.
    - HIPAA Technical Safeguard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.[ii]

d. *<The hospital>* will enforce encryption of all transmitted PHI. This requires that all employees use *<the hospital's>* secure text messaging applications for transmission of all text, video and picture-based PHI.
    - HIPAA Technical Safeguard: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.[ii]

SECTION 5: IT Involvement

<Hospital> IT will require access to device settings and configuration to support BYOD employees and implement the security measures outlined within section 4 for this policy. This access may be accomplished remotely or in person, including the use of Mobile Device Management (MDM) software. It is the goal of hospital IT to protect hospital data, while respecting employee privacy. This section of the policy outlines what IT will and will not support, what IT does and does not have access to, and what measures will be taken to preserve employee privacy.

5a) IT support

The following services are supported by the service/help desk:

a. Wi-Fi, email and VPN connectivity questions and configuration assistance.
b. Installation, updates and configuration assistance for hospital-related mobile applications, including:
    - Electronic Medical Records
    - Secure Text Messaging
c. Remote wipe for lost/stolen devices.
d. Spare/loaner device deployment and provisioning.

The following services are *not* supported by the service/help desk:

a. Device replacement.
b. Device upgrades.
c. Support of personal apps and settings.
d. Questions regarding device features and functionality.

Employees should contact the mobile service provider or device manufacturer for assistance with unsupported needs.

5b) IT access

<The hospital> will install Mobile Device Management (MDM) software on all devices that have accepted this policy and opted in the the BYOD program. This software will give hospital IT access to:

a. Enforce passcodes, encryption and settings restrictions.
b. Obtain an inventory of installed applications and device data.
c. Remotely wipe content from the device.
d. Push applications and settings to the device.
e. Disable features, such as the native camera on the device.
f. View web browsing history. Note: Though IT has access to browsing history, IT personnel will not be allowed to view this history unless there is a valid business (legal or regulatory) case.

IT will not have access to:

a. Track the location of the device.
b. See content within applications, pictures or videos.

5c) Employee privacy

<The hospital> will make every reasonable attempt to preserve employee privacy when enforcing this policy; however, by agreeing with this policy, the employee must waive the right to privacy when patient privacy is at stake. In order to preserve patient privacy and remain compliant with government regulations, the hospital must enforce certain security measures which may require that the hospital obtain access to locations where personal data is stored. The hospital's primary intention is not to impose on employee privacy, but to protect the patient's right to privacy.

The following are considered under the ownership of the employee and will not be accessed unless employee permission is granted or legal or regulatory requirement is imposed on the hospital:

a. The phone number of the device.
b. Personal text, picture, video and application content.
c. Phone contact lists.
d. Personal accounts that are set up on the device.
e. Device location.

SECTION 6: Penalties and Sanctions

Failure to comply with any of the requirements in this written policy may result in:

a. Termination of access to hospital resources.[i]
b. Termination of employment or other disciplinary actions.[i]
c. Civil or criminal prosecution.[i]

SECTION 7: User Agreement

I, _____, acknowledge that I have read and understand this policy and that I
(Participant Name)

agree with the terms and conditions. I will comply with the policy and accept any penalties (see

section 6) associated with non-compliance.

Participant Signature: _____

Date: _____

APPENDIX A: HIPAA Technical Safeguards

A covered entity or business associate must, in accordance with § 164.306:

(A)

(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)

(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)

(1) Standard: Transmission security. Implement technical security measures to guard against

unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) Implementation specifications:

(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Cited References

i Doheny R, Dulaney K, Wallin L-O. Toolkit: BYOD Mobile Device Policy Template. Gartner. https://www.gartner.com/doc/2659817/toolkit-byod-mobile-device-policy

ii. Summary of the HIPAA Security Rule. U.S. Department of Health & Human Services. http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations

Additional Reading

- 3-Part Guide to Developing a BYOD Strategy. Airwatch. http://www.air-watch.com/resources/white-papers/#3-part-guide-to-developing-a-byod-strategy

- Brown, N. BYOD in Healthcare: Creating a BYOD Policy. Nextech. http://www.nextech.com/blog/byod-in-healthcare-creating-a-byod-policy