KB0063394

Use of Personal Devices Policy

Swedish Medical Center (“facility”)

Department: Human Resources
Approved by: Chief Human Resources Officer
Date Last Reviewed: 1/15/2020
Date Last Revised: 1/15/2020
Date Adopted: 10/1/2019

Policy Name: Use of Personal Devices

Scope: All facility workforce members

Purpose: In keeping with our mission and values, the purpose of this policy is to provide guidance to workforce members concerning the use of personal devices.

Terms:

Jailbroken device: A personal device that has been modified to remove the controls and limits set by the original manufacturer.

Mobile card reader: The card reading device that connects to a tablet or phone.

Mobile point of sale (mPOS): Software that runs on a tablet or smart phone to conduct credit or debit card transactions.

Personal devices: Include, without limitation, cellular telephones, smart phones, electronic tablets/iPads, computers, and other electronic devices capable of wireless communication. This term includes workforce member-owned devices used to access company applications and data.

Workforce Members: Includes caregivers, volunteers, independent contractors, vendors, medical staff, interns, students or anyone else with access to the facility IS domain.

Policy:

1. Personal devices are an important method of communication and, at times, may be necessary to address safety, urgent business matters, or personal matters. The use of personal devices during work-related activities must conform to safety guidelines and common courtesy. In using personal devices, safety must come before all other concerns. Under no circumstances should workforce members place themselves or others at risk to fulfill work-related needs.
2. The use of personal devices during work-related activities must conform to facility policies and standards, including security, compliance, HIPAA, patient safety and social media.
3. A personal device is any device owned and paid for by the workforce member. It is the workforce member’s responsibility to use the personal device within these guidelines. The facility will not be liable for the loss or damage of personal devices brought into the workplace. As a courtesy to our workforce members, they may use their personal devices under the “Bring Your Own Device” (BYOD) program, as detailed below.
4. **Non-Exempt Workforce Members**. Non-exempt workforce members must not use personal devices for work purposes outside of their regularly scheduled work hours unless specifically authorized by their core

leader to do so. Workforce members must document in the timekeeping system any time they spend using personal mobile devices for work purposes to ensure they are paid for all time worked. Failure to comply may result in corrective action up to and including termination of employment.

5. **General Use of Personal Devices.** Calls from personal devices should not disrupt work duties. Workforce members should make sure conversations on personal devices are appropriate for the workplace, kept brief, and that patient confidentiality and privacy are maintained.
6. **Bring Your Own Device (BYOD Program):** The BYOD Program is a voluntary program intended to provide workforce members with the opportunity to use any personal device that the workforce member owns personally and access the facility systems (computer and network) in a secure environment, where the user logon is authenticated and data is protected. This may allow the workforce member to access email, calendars, contacts, to-do lists and other facility websites or data.
    A. **Approval of Device.** Workforce members who want to enroll in the BYOD Program must request enrollment through the Information Services department. Proper approval from the workforce member's department management and Information Services must be received. If the BYOD request is not approved, the workforce member will receive notification that the request has been denied. Enrollment requests will be approved or denied based on the following criteria, including but not limited to: business need for workforce member to use a personal device for work-related purposes, interference with job duties, compatibility with facility systems, etc.
    B. **Loss/Theft.** Any loss, damage or theft of a personal device is the sole responsibility of the workforce member. Personal device users must call the IS Service Desk immediately in the event that their devices have been lost or stolen so that appropriate security measures can be taken. The workforce member also agrees to immediately report any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of facility resources, databases, networks, etc.
    C. **Security.** Workforce members who use their personal devices to conduct facility business must adhere to the requirements in this policy.
        1. No confidential information may be copied/posted to unapproved 3rd party applications (e.g., Dropbox, Evernote, iCloud, etc.).
        2. Personally owned devices (e.g. camera, mobile phone, video recorder, tablet, and portable computer) are never to be used to photograph or videotape patients or patient information unless photos or videos are captured with Epic's Photo Capture Program via Haiku or Canto, or other secure mobile applications approved by Enterprise Information Security Governance.
    D. **Mobile Devices**
        1. Android or iOS devices that store facility data must be encrypted, unless the stored data is encrypted by a mobile application. Personally owned mobile devices are only allowed to connect to the BYOD-designated network or guest network.
        2. Mobile Device Management (MDM) is not required on personally owned devices when the device is using a facility security approved application that complies with the following controls (e.g., Microsoft Outlook, TigerConnect, Epic Canto, Haiku, or Rover):
            a. Password or PIN 6 digits in length or Biometrics
            b. Data encryption at rest and in transit
            c. The application must make data unreadable or inaccessible upon access revocation
        3. Prior to using a personal Android or iOS device to access facility systems or data, workforce members must agree to maintain enrollment within the facility standard Mobile Device Management (MDM) tool or suite of tools. The following device controls will be applied to a personally owned device:
            a. A facility device administrator will have the ability to apply appropriate device security controls.
            b. A password, PIN or biometrics will be enforced on the device.
            c. Device passwords or PIN will have a minimum length of 6 characters.
            d. Data on the device will automatically be erased after 10 failed authentication attempts or the device will lock out further authentication attempts.
            e. Device will be configured to password lock after a maximum of 5 minutes of inactivity.
            f. The device and/or data will be encrypted.
            g. Administrators have the ability to wipe data from personally owned devices.

E. **Laptops and Desktops.** Personally owned laptops or desktops are only allowed to connect to the BYOD-designated network or guest network and must have the following security controls in place:
    1. The device must have all available security patches installed (software and OS).
    2. The device must be configured to automatically apply critical patches (software and OS) at least weekly.
    3. The device must have an operable anti-malware program with current malware definitions installed, configured to update at least daily.
    4. Personally owned computers are not permitted to store facility data. They can only be used to access facility data via virtual environments like Citrix, VDI, or facility-approved cloud services.

F. **Reasonable and Appropriate Use of Personal Devices.** There are numerous personal plans for personal devices provided by various carriers. Workforce members are responsible for selecting the voice and data plan that best suits them and also allows for the extra voice and data related to the application used to access facility systems. It is the responsibility of workforce members to understand their voice and data plan, including the capabilities, costs and terms under the contract with the carrier. The workforce member's contract with the carrier is the responsibility of the workforce member. It is expected that workforce members will use their cell phones responsibly and in accordance with all applicable laws and facility policy. The facility reserves the right to apply uniform and consistently enforced controls over the application used to access the facility systems to the extent such controls are necessary to maintain production and discipline as permitted by law.

G. **International Calls.** If the workforce member uses the personally owned device on an official business trip internationally, the facility will reimburse the total amount of such international calls as provided for in the expense reimbursement policy.

H. **Ownership.** Personally owned devices remain the property of the workforce member. The workforce member owns the telephone number of a personally owned personal device. The data and information created with, transmitted by, and stored on personally owned personal devices by the application used to access facility systems is facility property.

I. **Privacy.** Workforce members have no expectation of privacy with respect to the application used to access the facility systems on a personal devices. Workforce members agree to and accept that their access and/or connection to facility networks may be monitored to record dates, times, duration of access, etc. The workforce member consents that there is no right to privacy related to use of organizational networks, resources, or data.

J. **Access to Information Services Systems.** Administrators may remove the personal device's access to our systems and data at any time. Upon removal of access, the facility data will be deleted from the device or rendered unreadable.

K. **Reimbursement.** Workforce members who are authorized to use a personal mobile device for work-related purposes may be eligible to receive reimbursement in accordance with the Expense Reimbursement policy.

L. **Credit/debit cards.** Personally owned devices and mobile card readers may not be used as mobile Point of Sale (mPOS) devices to conduct facility purchases.

M. **Malicious apps.** Caregivers may be required to remove malicious apps when detected in order to continue accessing facility data.

N. **Service Desk.** The Service Desk is only available to assist with issues directly related to our applications and data. Other issues are the responsibility of the workforce member.

O. **Liability.** While remote deletion due to separation of employment or lost device is intended for facility data, workforce members agree the facility will not be liable for any personal data deleted. Workforce members are responsible for backing up their personal data and ensuring no facility data is included in the backup.

P. **Legal discovery.** If used to conduct business matters, personally owned devices may be part of a legal discovery request. Workforce members may need to provide their personally owned devices to counsel. Subject to legal hold or preservation order, data on a personal device may be required to imaged or otherwise preserved.

Q. **Device sharing.** Personally owned devices with facility data may not be shared with other people including family members.

R. **Approval process**. Workforce members wishing to enroll their personal devices into the BYOD Program must first initiate a request through the Service Catalog or Service Desk. This request must include the Use of Personal Devices Acknowledgment and documented management approval before the request can be reviewed for appropriateness and implemented.

Procedures:

1. Prior to using personal devices for email or facility related applications, workforce members must agree to the “Use of Personal Devices Acknowledgment”.
2. If a personal device is lost or stolen, the personal device user must call the IS Service Desk immediately so that appropriate security measures can be taken.
3. When a workforce member departs the facility, all facility related data will be securely deleted using standard Information Services procedures and technologies. Workforce members are required to permanently delete any facility data that was not addressed by Information Services.

Help: For questions about this policy, or assistance with understanding your obligations under this policy, please contact human resources.

The statements of this policy document are not to be construed as a contract or covenant of employment. They are not promises of specific treatment in specific situations and are subject to change at the sole discretion of the facility.

This policy does not modify the express terms of any collective bargaining agreement. In the event of a conflict between this policy and the terms of a collective bargaining agreement, the collective bargaining agreement will prevail.

Use of Personal Devices Acknowledgment

The use of any personal device for work purposes, whether during working or non-working hours and whether on or off facility premises, must conform to the terms set forth in the Use of Personal Devices and other facility policies. I acknowledge the risks associated with the use of my personally owned and/or facility issued device for work purposes, and I consent to facility controls and technical enhancements designed to protect the facility and its information, networks and data.

Terms and conditions

I agree to the following terms and conditions.

1. I have voluntarily elected to use a personal device for the purpose of conducting facility work, in addition to personal usage during non-work time.
2. I understand that use of facility managed applications on a non-facility devices will have security controls enforced on the managed applications.
3. For personally owned devices that are required to be managed by the Mobile Device Management system, I acknowledge that the facility will enforce security settings on my mobile device including, encryption, PIN, passcode or Biometric authentication, timeout setting and lockout or wipe my device after 10 failed login attempts.
4. If needed for an investigation, the personal device will be provided for the facility to access facility data on the device.
5. If eligible, the facility will provide a mobile device for the purpose of conducting work activities.
6. I will use my personal device in compliance with all applicable facility policies.
7. I understand Microsoft Exchange^{TM} mailbox information is maintained and backed up by the facility and should not be replicated onto non-facility

8. I will use my personal device in compliance with all applicable laws and ordinances, including any laws that limit or prohibit the use of a mobile device while driving.
9. I understand that failure to adhere to these conditions or failure to appropriately safeguard facility information could result in action against me, including termination of employment, civil action, or criminal prosecution.
10. I agree to hold the facility harmless for any loss relating to the administration of my mobile device connectivity to facility systems including, but not limited to, loss of personal information stored on a mobile device.
11. I agree to have my mobile device wiped by the facility upon request by the facility.
12. I understand the facility may at any time and without my prior notice or consent, change or terminate the Bring Your Own Device (BYOD) program.
13. I understand and agree that if I am a workforce member who is eligible to receive overtime pay, that this policy is not actual or implicit approval from the facility for me to perform work remotely instead of in my designated workplace. If special permission or approval is required for me to perform work other than in my designated workplace and during designated work times, I will obtain prior approval from my core leader.

Acceptance acknowledges that I have read the Use of Personal Devices policy and that I will comply with its requirements.