Jefferson

Policy No: **102.35**
Original Issue Date: 1/20/2007
Review Date: 7/17/2015
Revision Date: 7/17/2015

**HOSPITAL POLICIES & PROCEDURES**

| | |
|---|---|
| Category: | Administration |
| Title: | **Jefferson Mobile Device Policy** |
| Applicability: | Thomas Jefferson University Hospitals, Inc. |
| Contributors/Contributing Departments: | Information Services & Technology and Payroll |

## PURPOSE

The purpose of this policy is to provide general guidelines regarding the use, procurement and issuance of a corporate mobile device or a corporate managed personal device. This policy will also outline the general guidelines for qualifying for and receiving reimbursement of expenses associated with a corporate managed personal device.

## DEFINITIONS

1. Mobile Device
    a. Unless otherwise specified, the term "mobile device" throughout this document refers to a cell phone, smartphone, tablet or laptop device with cellular or Wi-Fi coverage.
2. Corporate Issued Mobile Device
    a. All mobile devices that are issued and paid for by Jefferson under the corporate contract.
3. Corporate Managed Personal Mobile Device
    a. A mobile device, being used to send or receive Jefferson data and that has Jefferson security software and policies applied, that is being paid for by the individual under a personal contract with a service provider. While Jefferson workforce members may be eligible for discount plans from a number of providers, the workforce member assumes full liability for these devices and plans.
4. Shared Device
    a. A Corporate Issued Mobile Device procured for requests where the mobile device is passed from shift to shift. The mobile device cannot be routinely carried or used by a single workforce member.

## POLICY

Corporate Issued Mobile Devices are intended for the sole use of conducting Jefferson business. Corporate Managed Personal Mobile Devices, though used for both personal and Jefferson business, will comply with all Jefferson policies and procedures and will maintain all security software while they are used to conduct Jefferson business. All workforce members eligible for and approved for corporate managed personal mobile devices, which are to be used for Jefferson business, may be reimbursed an amount equal to the cost paid by Jefferson for a corporate issued mobile device.

## ELIGIBILITY FOR A CORPORATE MANAGED PERSONAL MOBILE DEVICE

In order to justify the need for a Corporate Managed Personal Mobile Device, a workforce member

needs to meet both of the following criteria:

- Critical Operations: The workforce member is required to be immediately available by telephone, both during and outside normal business hours, for clinical and administrative decisions.
- Mobility: A workforce member is required to be immediately accessible for work related purposes, is away from the member's primary office phone longer than 50% of the time and alternate communication methods are deemed insufficient.

**ELIGIBILITY FOR A CORPORATE ISSUED MOBILE DEVICE**

In order to justify the need for a Corporate Issued Mobile Device, the employee using the device needs to meet both of the following criteria:

- Critical Operations: The workforce member is required to be immediately available by telephone, both during and outside normal business hours, for clinical and administrative decisions.
- Mobility: A workforce member is required to be immediately accessible for work related purposes, is away from the member's primary office phone longer than 50% of the time and alternate communication methods are deemed insufficient.

**Workforce Member's Responsibility**

- All corporate issued or corporate managed personal mobile devices that are used to process, transmit, store or access Jefferson information are required to have the Jefferson security software and policies applied to them.
  - An End User Responsibility Statement must be signed at the time the mobile device is configured with the above software and the workforce member is required to be familiar with all documented expectations, including familiarity with all applicable Jefferson policies and procedures, indicated in the End User Responsibility Statement.
  - Workforce members must check with the Information Services & Technology (IS&T) Customer Service Center (CSC) to validate Jefferson's current **list of supported devices** ***before*** upgrading or replacing a corporate managed personal device.
  - Unsupported devices will *not* be eligible for use as a Corporate Managed Personal Mobile Device, will not receive the Jefferson security software, and therefore may not be used to conduct Jefferson business.
- In the event the workforce member upgrades or replaces a corporate managed personal device, he or she is required to contact the IS&T Customer Service Center to have the Jefferson security software configured on the new or upgraded mobile device.
- If the workforce member chooses to use a personally owned mobile device to support on-call responsibilities, the workforce member is still required to be available in accordance with the expectations set forth by their department without exception.
- All workforce members are responsible for the care and safekeeping of all mobile devices and the data on each device.
  - All workforce members required to be on-call or to be immediately available for making critical clinical or administration decisions must maintain the mobile device to ensure its reliability. In the event the mobile device is damaged, lost or stolen, the workforce member is responsible for securing a replacement in a timeframe consistent with the demands of his or her position. Alternate contact methods must be made in the interim and communicated to the appropriate individuals.
- Mobile devices should NOT be used as an alternative to regular Jefferson "wired" telephone service.

- Corporate issued mobile devices should not be used for personal purposes.
    - Call usage reports should be reviewed annually to ensure that personal usage is nominal.
- All workforce members are responsible for adhering to all applicable local, state and federal laws and regulations related to the use of mobile devices.
- Do not use mobile devices while driving or operating other equipment, unless extreme safety precautions have been taken.
- Patient Confidentiality and Privacy policies apply when using the mobile device.
- The workforce member may be responsible for the cost of replacing a mobile device that is lost, stolen or misused. The department head will make the determination based on information obtained from IS&T concerning the identified state of the phone and cost to replace the phone.
- Workforce members must notify their direct manager and IS&T immediately, should they discontinue their personal mobile device service.
- Workforce members are responsible for full support of their mobile device, with the exception of configuration of Jefferson security software and connectivity to approved Jefferson applications and services.
- Should the workforce member transfer to a position outside his or her current department he or she is responsible for requesting permission to continue receiving the benefit of a corporate managed personal device.
- Workforce members must share the phone number associated with any corporate managed personal mobile device with all appropriate individuals within Jefferson.
    - The mobile device number will be automatically entered into any corporate communication tool identified as a key operational resource to the workforce member's position.

**Management Responsibility**

- Management is required to ensure that the workforce member is aware of the policies, procedures and expectations regarding the use of the mobile device, and the importance of adherence.
- Management is required to ensure, where possible, that mobile devices are shared with other workforce members in the department.
- Management must perform an annual audit to ensure that all workforce members with corporate issued or corporate managed personal mobile devices are still eligible to have them.
- Management will receive an email requesting approval for any workforce member requesting a corporate issued mobile device or the use of a corporate managed personal device. Management is required to respond by either denying the request or approving the request with an attestation that the workforce member is required to be immediately available for clinical or administrative decisions and that they are away from their office phone for longer than 50% of the time.
    - If management is approving a corporate managed personal device and feels that the workforce member is eligible for reimbursement of any personal service fees they incur, management may indicate in the email an amount to be reimbursed – not to exceed the cost paid by Jefferson for a corporate issued mobile device.
- All mobile device documentation is subject to review by the responsible department, by Financial Administration and by Internal Audit. All supporting documentation related to the reimbursement of mobile device expenses must be maintained in the department for three years.
- Policy contributors will review the policy periodically and communicate any changes to all eligible workforce members.

## PROCEDURE

**PROCUREMENT**

- Requests for mobile devices and associated accessories, configuration of corporate managed personal devices and all changes to services (text packages, data service, international roaming,

etc.) must be made through the IS Request Tracking System (http://myrequests.tjuh.org).
    - The IS&T CSC will obtain approval from the workforce member's Vice President or Administrator.
- Requests for new devices are ordered by the IS&T CSC and are available in accordance with the SLA outlined in the IS&T service catalog.
- Jefferson workforce members who are not designated approvers of Information Services and Technology are not permitted to enter into a mobile contract or agreement for mobile service on behalf of Jefferson.
- The IS&T CSC will support all corporate issued mobile devices and provide technical support, training, and consultation, upon request.
- The IS&T CSC will configure Jefferson's security software on all approved corporate managed personal mobile devices.
- To obtain a current listing of supported mobile devices, contact the IS&T CSC, or **click here**.

**Original Issue Date:** 1/20/2007
**Revision Date(s):** 3/12/2009, 3/12/2011, 08/06/2013, 7/17/2015
**Review Date(s):** 3/12/2009, 3/12/2011, 08/06/2013, 7/17/2015

**Responsibility for maintenance of policy:** Vice President, Infrastructure & Architecture Design

(Signature on File)

**Approved by:**
Richard J. Webster, MSN, RN, NEA-BC
President,Thomas Jefferson University Hospitals, Inc.