Duke Health Policy: Use of Personal Mobile Devices [1]

Version 1.0

Note: The following information is provided here for convenience. The authoritative version of Duke Heath’s Use of Personal Mobile Devices policy can be found on the Duke Health Policy Center web site [2]. Additional background and tips can be found on the Duke Health Mobile Device Manager web site [3].

Authority

Duke Health Chief Information Officer
Duke Health Chief Information Security Officer

Policy Statement

Duke Health recognizes that the use of Personal Mobile Devices can be a valuable tool in conducting the business of the organization. However, members of the Duke Health Enterprise Workforce who wish to use a Personal Mobile Device must exercise care to ensure that these devices are used in a way that minimizes the risk of a security or privacy breach. Furthermore, Duke Health must respect the privacy of individual members of the Workforce by limiting its monitoring and management capabilities to only those functions approved through information technology and information security governance processes. The following policy statements provide the requirements for fulfilling these obligations.

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>

| **Duke Health Enterprise (DHE)** | DHE includes Duke’s Affiliated Covered Entity (ACE) and the Organized Health Care Arrangement (OHCA) that covers the following entities: Duke University Health System, Duke University Hospital, Duke Connected Care, Duke Regional Hospital and corresponding medical staffs, Duke Raleigh Hospital and corresponding medical staffs, Duke University Affiliated Physicians (aka Duke Primary Care), Private Diagnostic Clinics, Duke Home Care and Hospice, Associated Health Services, Inc., (dba Davis Ambulatory Surgical Center), Patient Revenue Management Organization, LLC, Duke University School of Medicine, Duke University School of Nursing, Duke Clinical Research Institute, Sexual Assault Support Services, Personal Assistant Services, Counseling and Psychological Services (CAPS), Duke University Student Health, Duke University Police Department, and Live for Life. |
| **Duke Health Enterprise Workforce** | Employees, medical staff members, faculty, students, volunteers, trainees, third party consultants, vendors, service providers, or other contractors whose conduct, in the performance of work for a covered entity is under control of such entity, whether or not they are paid by the DHE. |
| **Duke Health Wireless Network** | Connects to the Duke Health wired network behind the Duke Health firewall, is for use only by the Duke Health constituency, and is defined in the Duke Health Wireless Network Standard. |
| **Enterprise Container** | A virtualized portion of a device or system which is designated as holding Duke Health managed applications and data. |
| **Personal Mobile Device** | Any mobile phone, smartphone, or tablet device that is owned, leased, or otherwise provided by an individual member of the Duke Health Enterprise Workforce, and is used to access, store, or process Duke Health systems, applications, data, or other IT resources. |
General Conditions and Eligibility

- Duke Health expects Users to assume certain responsibilities for any Personal Mobile Device that contains enterprise information or connects to enterprise resources. Users must ensure that they comply with all sections of this policy, as well as complementary policies and agreements such as, but not limited to the Duke Health Confidentiality Agreement and the Mobile Computing and Storage Device Policy, the Mobile Computing and Storage Device Standard, and the Duke Health Secure System Usage Memo.
- Users wishing to use a Personal Mobile Device for Duke Health business must agree to enroll the device with the Duke Health Mobile Device Manager. This will install a software agent on the device that will enable Duke Health to manage certain aspects of the device.
- Enrolling a Personal Mobile Device with the Duke Health Mobile Device Manager will create an Enterprise Container that is remotely managed by Duke Health. The Enterprise Container enables Duke Health applications and data to be stored and managed separately from personal applications and data on the device. Under certain circumstances, such as the User’s separation from the Workforce or the loss or theft of a Personal Mobile Device, the Enterprise Container may be remotely deleted by Duke Health. Wiping the Enterprise Container from the device should have no effect on any personal applications or data stored on the device.
- Users must maintain a Mobile Device that is compatible with Duke Health’s Mobile Device Supported Platforms Standard, including but not limited to hardware and operating system versions. Users must apply all software updates, which may be supplied by the device manufacturer, telecommunications provider, Duke, or third party developers, in a timely fashion. If a device falls out of compliance, then it may be blocked from access until it meets the minimum requirements.
- The use of a Personal Mobile Device is considered a privilege meant for the User’s convenience. Duke Health reserves the right to rescind this privilege without notice.
- Duke Health takes no responsibility for damages to hardware or loss of personal data that may occur during the course of using a Personal Mobile Device. Duke Health recommends that the User maintain current backups of any personal data, and, as appropriate, maintenance contracts or insurance policies to cover potential damages. Users must accept that they are solely responsible for backing up any personal applications and data on their Personal Mobile Device.
- For members of the Workforce who are considered Non-Exempt under the U.S. Fair Labor Standards Act: when using a Personal Mobile Device to conduct enterprise business on behalf of Duke Health, the User agrees to limit his or her reading of, and response to, enterprise email, text messages, phone calls, and other forms of corporate communications to predetermined and regularly scheduled business hours. The use of a Personal Mobile Device is voluntary, and by no means constitutes a request by Duke Health, direct or implied, to conduct enterprise business on the personal mobile device outside of predetermined and regularly scheduled business hours.
- Reimbursement of expenses incurred by Users for the use of a Personal Mobile Device will
follow their departmental policies. In general, if a stipend is provided to allow the User to purchase a Personal Mobile Device, then the device must be enrolled with the Duke Health Mobile Device Manager.

**User Privacy**

- Duke Health takes protecting the privacy of its Workforce seriously. Although the Mobile Device Management software installed on a User’s Personal Mobile Device provides Duke Health with limited abilities to remotely monitor and manage certain aspects of the device, it does not provide Duke Health with access to the personal data that is stored outside of the Enterprise Container on the device.
- Unless required by a lawful request as described under the Preservation Notices and E-Discovery section of this policy, Duke Health will not access sensitive personal information stored on a Personal Mobile Device, including but not limited to geographic location, SMS texts or logs, browser activity, social media accounts, application profiles, keystroke activity, personal email, personal calendar, and personal contacts. Duke Health has put in place appropriate technical and administrative controls to restrict access to sensitive personal information.
- Any changes to this policy or accompanying standards that may affect user privacy must be approved by, at minimum, the Duke Health Privacy and Security Steering Committee (PSSC) and the Duke Health Information Technology and Informatics Oversight Committee (ITIOC).

**Applications and Downloads**

- Duke Health mobile applications will be made available for download through a Duke Health App Store that is provided through the Duke Health Mobile Device Manager. These applications are subject to policies described in this document about data/applications, and will be stored in the Enterprise Container. As a general rule, mobile applications that may be used to download or store PHI onto a mobile device should be managed through the Duke Health App Store.
- Users may download and install additional applications from the platform’s public application store (e.g., Apple App Store, Google Play). Users are advised not to download applications from non-public stores due to a lack of security review for these applications and the greater potential for compromise of the device.

**Security, Functionality, and Feature Management**

- In accordance with the Duke Health Mobile Computing and Storage Device Policy and Standard, the following basic security controls will be enforced on Personal Mobile Devices through the Duke Health Mobile Device Manager:
  - Use of a passcode with a minimum of 4 digits. Alphanumeric passcodes with 6 or more digits are preferred. When available and supported by the Duke Health Mobile Device Manager, the use of biometric access protections such as TouchID are permitted and encouraged.
  - Full encryption of the device and all attached storage (e.g. SD cards). In cases where this is not technically feasible, encryption of the Enterprise Container may be
acceptable if it can be guaranteed that no Duke data will be written outside of the container. See the Exceptions section of this policy for further information on how to request a policy exception for these cases.

- Autolock of the device after no more than 5 minutes of inactivity.

- Using Personal Mobile Devices that have been “jailbroken,” "rooted,” or have otherwise been subjected to any other method of altering or disabling built-in protections is not permitted. The Duke Health Mobile Device Manager will not permit the enrollment of jailbroken or rooted devices. If a Personal Mobile Device is jailbroken or rooted after enrollment, the device will be considered out of compliance and the Enterprise Container will be remotely wiped from the device, and the device will no longer be allowed to connect to the Duke Health network.

- Cameras and microphones in mobile devices are to be used in accordance with the Duke Health Patient Photography, Video, and Audio Recording Policy [9].

**Wireless (WiFi) Networks**

- In order to be eligible to connect to a Duke Health Wireless Network (e.g. "clubs"), a Personal Mobile Device must be enrolled with the Duke Health Mobile Device Manager. Failure to enroll may result in the loss of ability to connect a device to the Duke Health Wireless Network.

- Users should exercise care when connecting to unfamiliar, unsecured public WiFi networks, such as those found in coffee shops, airports, and hotels. Whenever possible, Users should opt to use the cellular network or a personal WiFi hotspot instead of a unsecured public WiFi network. More information on this topic can be found in the Duke Health Secure System Usage Memo [8].

**Physical Protections**

- Users must take precautions to prevent the theft of their Personal Mobile Devices, as well as accidental disclosure of Duke data that may be accessed from or stored on their Personal Mobile Devices. Devices should not be left unattended in a visible public location, such as an unattended vehicle, an office or room with a street-level window, a co-working space, or a restaurant.

- A Personal Mobile Device displaying sensitive information being used in a public place (e.g., in an aircraft, public transportation, or coffee shop) must be positioned so that the screen cannot be viewed by others. A tinted or polarized screen guard may be used to decrease the viewing angles of any mobile device.

- Users must take appropriate precautions to prevent others from obtaining access to their Personal Mobile Device. Users will be responsible for all transactions made with their credentials, and will not share individually assigned passcodes or other access credentials.

**Loss or Theft**

- Users must report the loss or theft of Personal Mobile Devices to the Duke Health Service Desk at 919-684-2243 or the Duke Health Information Security Office via email to security@duke.edu [10]. This report should be filed as soon as possible after the incident, and no more than within 24 hours of the incident. If theft is suspected, a report must also be
filed with the local law enforcement authority; for theft incidents on campus, Duke University Police Department should be contacted at 919-684-2444.

- The Duke Health Information Security Office will evaluate the circumstances around the loss or theft to determine the risk of a data breach. Based on the results of that evaluation, a command may be issued to remotely wipe the Enterprise Container from the device. The User will also have the option of issuing a command through the Duke Health Mobile Device Manager to wipe the entire device.
- Additional steps and details that should be followed in case of the loss or theft of a Personal Mobile Device are documented in the following Knowledge Base article: https://duke.service-now.com/kb_view.do?sysparm_article=KB0019837

**Device Replacement, Upgrade, and Termination of Service**

- Users must un-enroll their Personal Mobile Devices before replacing, upgrading, or terminating service with a wireless carrier. Un-enrolling the device will cause the Enterprise Container, and the associate Duke Health data and apps, to be removed from the device.

**Termination of Employment**

- Upon termination of employment, Duke Health will remotely remove the Enterprise Container that houses Duke Health data and applications. In certain situations, Duke Health may also request that a User must confirm, in writing, that they have removed all Duke Health data from their Personal Mobile Device, as well as any online or offline backups of such data. If the User fails to remove Duke Health data and applications from a Personal Mobile Device upon Duke Health's request, then Duke Health may pursue legal remedies against the User.
- Former members of the Workforce are not authorized to restore any application or data that originated through the relationship with Duke Health. Any attempt to restore such information may be subject to legal action against the former employee.

**Preservation Notices and Electronic Discovery (E-Discovery)**

- From time to time, members of the Workforce are subject to legal actions related to their work at Duke Health and, as a result, may receive a preservation notice, also sometimes referred to as a legal hold, from Office of Counsel instructing them to preserve electronic data associated with a particular matter. Users are responsible for fulfilling the obligations stated in the preservation notice, and should assess whether a Personal Mobile Device may contain data associated with the legal matter that is the subject of the notice.
- If the User determines that data associated with the legal matter is stored on a Personal Mobile Device, it is the User’s sole responsibility to ensure that a copy of that data is maintained in case it is requested as part of a future e-discovery request. Such data must be preserved until such time that Office of Counsel issues a release of preservation notice. Note that if the User leaves the Workforce before a release is provided, the User remains responsible for preserving the data or providing Duke Health with a copy of the data.
- In the unlikely event of Duke Health or Duke University being required under court order to access to a Personal Mobile Device for lawful e-discovery purposes, Users are obliged to provide reasonable access to the device along with the necessary passcodes in
accordance with applicable local, state or federal laws. Such requests will only be made through the Office of Counsel and with the explicit approval of the Duke University and, if applicable, Duke University Health System Executive Vice Presidents. As permitted by law, users will be notified of any such requests before they are fulfilled, and will have the right to contest such requests by working with the Office of Counsel.

- Questions regarding preservation notices and e-discovery requests, including concerns around the proper procedures for handling data that is part of a legal matter, should be addressed to the Office of Counsel as noted in the preservation notice or e-discovery request.

**Administrative Access**

- Administrative access to the Duke Health Mobile Device Manager will be tightly controlled by Duke Health Technology Solutions (DHTS). Only IT support staff who have a legitimate business reason will be granted administrative access. All requests for administrative access must be reviewed and approved by the Duke Health Chief Information Security Officer before being granted.
- Those with administrative access to the Duke Health Mobile Device Manager will be held to the highest ethical standards by DHTS leadership. Anyone who is found to be misusing their privileges to access private information about Users or change settings on Personal Mobile Devices without permission will be subject to HR action in accordance with sanction policies.
- As a general course of business, administrative access will be automatically disabled upon an administrator’s employment separation from Duke. or upon a job role change that no longer requires the access. In addition, on not less than an annual basis, an audit will be performed by the Information Security Office and the Duke Health Mobile Device Manager Service Owner to review administrative access and remove individuals who should no longer have access.

**Effective Date of Policy:** 08/01/2017

For additional information, please visit [https://mobile.dhts.duke.edu/](https://mobile.dhts.duke.edu/) [3]