SUNY DOWNSTATE MEDICAL CENTER

UNIVERSITY HOSPITAL OF BROOKLYN
POLICY AND PROCEDURE

Subject: **MOBILE DEVICE USAGE**

No. HIS-12

Page 1 of 4

Prepared by: Information Security Officer

Original Issue Date: 6/2013

Supersedes: NEW

Reviewed by: John Dooley, DMC, CIO
Shoshana Milstein
Alan Dzija, DMC, CFO

Effective Date: 6/2013

TJC Standards: IM01.01.01, IM.02.01.03, IM.02.01.01,

Approved by: Margaret Jackson, MA, RN
David Conley, MBA
Marwan W. Atallah, M.D.
Michael Lucchesi, M.D.
Alan Dzija, DMC, CFO
George P. Carafis, MBA

Issued by Regulatory Affairs

I. POLICY

This policy applies to all SUNY Downstate Medical Center (SUNY DMC) employees, faculty, staff, residents, students, contractors, consultants, temporary workers, and other authorized third party entities and personnel (herein referred to as "workforce members"). The use of mobile devices may be allowed for conducting SUNY DMC business operations. It is recognized that mobile devices are widely used but associated risks are high so they must be used in an appropriate, professional and businesslike manner in accordance with the guidelines specified in this mobile device usage policy.

II. PURPOSE

Mobile devices may be allowed for use at SUNY DMC for business purposes related exclusively to the scope of each person's employment or other relationship with SUNY DMC only when there is a legitimate business reason and when a reasonable alternative (for example VPN or other remote access) is impractical or does not exist. All emails, text messages, files, and photos related to SUNY DMC that are created, sent, received, stored or accessed on any mobile device shall be treated as business messages or files. Accordingly, all users shall have *no expectation of privacy* related to any message or file created, sent, received, or stored on a mobile device. SUNY DMC reserves the right to access any or all of these messages or files at any time pursuant to compliance, regulatory, legal, or other factors deemed appropriate by management.

Mobile devices used to create, send, receive, store, and access electronic Protected Health Information (ePHI) are subject to special requirements designed to minimize the risk of inappropriate disclosure of ePHI through theft or accidental loss.

Effective security is a team effort involving the participation and support of every SUNY DMC workforce member and affiliate who is a user of SUNY DMC information on mobile devices. It is the responsibility of every user to know these guidelines and to conduct their activities accordingly.

III. DEFINITIONS:

a. *Computer System*: refers to the DMC center-wide network. The Computer System includes, but not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, web servers.

b. *Electronic mail (e-mail):* refers to any message, image form, attachment, data, or other communication sent, received, or stored within all electronic messages sent or received on the SUNY DMC ***Lotus Notes*** messaging system.

c. *Users or Workforce Members:* refer to all employees, faculty, staff, residents, students, independent contractors, consultants, temporary workers, and other persons or entities who utilize SUNY DMC's Computer System.

IV. SCOPE

This policy applies to all mobile devices that are owned by SUNY DMC as well as those mobile devices that are not owned by SUNY DMC (i.e. personally owned) but are used to access the SUNY DMC network, data and systems or create related content.

Types of mobile devices covered by this policy include but are not limited to:

- Laptop and notebook computers
- Cell phones and smart phones
- Tablets (e.g. iPads)
- USB drives (e.g. thumb drives, external hard drives)

V. PHYSICAL SECURITY

a) The user of a mobile device must provide reasonable safeguards and manage the location of the device to prevent unauthorized access. These measures must be commensurate with the data criticality and risk.
b) In the case of a mobile device reported lost or stolen, SUNY DMC has the right to remotely delete all data therein and disable the device accordingly.
c) Physical security is the responsibility of the device owner, who is also responsible for appropriate disposition of the device when it is retired from use, including the permanent deletion of all DMC related content. For disposal of DMC issued mobile devices, the Computer/ Electronic Waste Procedure must be followed (available on the DMC IS website at http://is.downstate.edu).
d) Lost mobile devices must be reported immediately to the SUNY DMC Information Security Officer (ISO) by contacting the IT Service Delivery & Customer Support Center at extension 4357 (HELP), the DMC Compliance Line at 1-877-349-SUNY or by making a web report by clicking the "Compliance Line" link on the bottom of DMC's webpage.

e) Personally owned mobile devices may be subject to seizure in the event of a security related incident.

VI. LOGICAL SECURITY

a) Passwords must be used on mobile devices. On laptops, notebooks, and tablets, passwords and related settings should meet the password requirements for all SUNY DMC computers (See HIS-04, Password Policy, available on the DMC IS website at http://is.downstate.edu). On cell phones and smart phones, passwords are required to be at least four digits.
b) Mobile device management software will be installed by SUNY DMC on each mobile device as deemed appropriate by management.
c) Mobile devices may be wiped (i.e. contents deleted) whenever deemed necessary by SUNY DMC and without the consent of the user.
d) Mobile devices must not be "jail broken" or "rooted" by the user.
e) Software or firmware designed to access functionality not intended to be exposed to the user may not be installed on mobile devices.
f) Pirated software or illegal content may not be loaded on the mobile devices.
g) USB drives and portable devices are only authorized for the temporary, on- site storage or file sharing of ePHI between authorized users. The ePHI must be deleted as soon as the business purpose has been accomplished and cannot be removed from SUNY DMC premises. Drives and portable devices containing ePHI that are taken off- site must meet SUNY DMC encryption standards. Long term or permanent storage of files containing ePHI must also meet SUNY DMC encryption standards.
h) Patient images captured using the camera on mobile devices should immediately be uploaded to the SUNY DMC network by email or USB transfer to an appropriate non-mobile device (e.g. desktop computer, network storage drive) and deleted from the mobile device.
i) Security patches and updates should be downloaded and installed as soon as they are made available for the mobile device.
j) Mobile devices with SUNY DMC files or information should not connect to unsecured wireless networks.

VII. ADMINISTRATION

a) Each user must sign a Mobile Device Understanding form before using a mobile device for ePHI.
b) To ensure appropriate use of mobile devices, SUNY DMC may monitor their use as deemed appropriate by management.
c) All violations of this policy will be investigated and documented by the ISO or his/her designee, including complaints alleging a breach of confidentiality, code of conduct violation, abuse or unacceptable use of mobile devices. All investigations of violations will be provided to the SUNY DMC ISO and disciplinary action may be taken against the individual(s) involved.
d) All emails used to communicate between providers and patients must be in accordance with this policy and with DMC's Email Policy.
e) SUNY DMC reserves the right to review, audit, intercept, access and disclose all files and messages created, received, sent, accessed, or stored by mobile devices.
f) Under certain circumstances, the system administrator(s) may, in the course of his or her professional duties, access an individual's mobile device for legitimate management or maintenance purposes. System administrators will not purposely read the contents of messages or other information. Additionally, the ISO may access an individual's mobile

device for law enforcement purposes.

VIII. ENFORCEMENT

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or any other relationship with DMC.

Disciplinary actions taken will be determined dependent on the circumstances of the violation. Particular measures will be used to establish appropriate disciplinary action, including:

1. Whether the violation was negligent or intentional;
2. Whether the violation was isolated or repeated;
3. The nature and extent of harm caused by the violation;
4. Whether the violation involved personal gain;
5. Whether and to what extent the person assisted to discover and remedy the violation;
6. The hierarchical level and degree of discretionary authority of the offender; and
7. Whether lesser or alternative forms of redress fully address the violation and meet the goals of this policy.

IX ATTACHMENTS:

Mobile Device Understanding Form

X. REFERENCES:

- Joint Commission Standards
- HIPAA Privacy & Security Rules

XI. REVISION HISTORY

Date Reviewed	Revision Required (Circle One)		Responsible staff Name and Title
	Yes	No	
	Yes	No	
	Yes	No	
	Yes	No	
	Yes	No	

SUNY DOWNSTATE Medical Center

MOBILE DEVICE UNDERSTANDING FORM

I have read and understand the SUNY Downstate Medical Center (DMC) Mobile Device Usage Policy and its requirements, which include but are not limited to:

1. Using reasonable and appropriate safeguards at all times, including whether on- site or off-site, to protect the confidentiality and to prevent unauthorized access of SUNY DMC related data on mobile devices.
2. Using at least a four digit password on my cell phone/smart phone if it is used in any way for SUNY DMC business.
3. Using USB drives and portable devices only for temporary, on- site storage or sharing of ePHI between authorized users and deleting the information as soon as the business purpose has been accomplished. Patient images taken with a mobile device will be immediately uploaded to SUNY DMC's network and the images will be deleted from the device before going off- site.
4. Not removing USB drives and portable devices containing ePHI from SUNY DMC premises unless the data is encrypted in accordance with SUNY DMC encryption standards.
5. Not transmitting ePHI over the Internet unless the data is encrypted in accordance with SUNY DMC encryption standards.
6. Not using USB drives and portable devices for long term or permanent storage of ePHI unless the drives and devices meet SUNY DMC encryption standards.
7. Keeping up- to- date with security patches and updates for mobile devices.
8. Properly disposing mobile devices when they are retired from use, including following SUNY DMC procedures for SUNY DMC issued devices.
9. Immediately reporting lost or stolen mobile devices that have been used for SUNY DMC business in any way.
10. Immediately reporting a breach or potential breach of any mobile device that has been used for SUNY DMC business in any way, including unauthorized access to ePHI contained on the mobile device.

** Reports should be made to the IT Service Delivery & Customer Support Center at extension 4357 (HELP), to the DMC Compliance Line at 1-877-349-SUNY or by making a web report by clicking the link "Compliance Line" on the bottom of DMC's webpage.

I also understand that if I choose to use my personal mobile device to access SUNY DMC email or for other SUNY DMC business purposes, all of the data on the mobile device (business and personal) may be deleted when deemed necessary by SUNY DMC management.

Workforce Member Name	Workforce Member Signature	Date