SUNY Downstate Medical Center

College of Medicine
School of Graduate Studies
College of Nursing
College of Health Related Professions

IT Service Delivery & Customer Support Center

Downstate Owned Mobile Device Consent Form

User Name: _____ User Title: _____

DMC ID #: _____ User Contact Number: _____

User Downstate Email Address: _____

Name of Department Chair/ Director: _____

Name of Department Administrator/ Supervisor: _____

DMC Mobile Device Information	
Device Manufacturer	
Model	
Serial Number	
Device Manufacturer	
Model	
Serial Number	
Device Manufacturer	
Model	
Serial Number	

I have read and understand the SUNY Downstate (DMC) Mobile Device Usage Policy and its requirements and agree to the terms and conditions therein. These requirements 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 DMC related data on DMC mobile devices.
2. Using a password that is:
    a. No less than eight (8) characters in length;
    b. Contains a minimum of three of the following four characteristics:
        - ✓ Uppercase English letters (A - Z)
        - ✓ Lowercase English letters (a - z)
        - ✓ Numbers (0 through 9)
        - ✓ Special Characters (space, !@#$%^&*-+/~,)

3. Using the DMC mobile device only for temporary, on- site storage or sharing of DMC related files between authorized users and deleting the information as soon as the business purpose has been accomplished. Patient images taken with a DMC electronic device must be immediately uploaded to DMC's network and the images must be deleted from the device before going off- site.
4. Not removing the mobile device containing DMC related data from DMC premises unless the data is encrypted in accordance with DMC encryption standards.
5. Not using the mobile device for long term or permanent storage of DMC files unless the drives and devices meet DMC encryption standards.
6. Keeping up- to- date with security patches and updates for mobile devices.
7. Properly disposing mobile devices when they are retired from use, including following DMC procedures for the DMC owned devices.
8. Immediately reporting lost or stolen mobile devices that have been used for DMC business in any way.
9. Immediately reporting a breach or potential breach of any mobile device that has been used for DMC business in any way.

** Reports regarding lost or stolen devices 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 the DMC owned mobile device for other personal, non- DMC business purposes, all of the data on the mobile device (business and personal) may be deleted when deemed necessary by DMC management.

I understand that this policy agreement and the privilege to use such mobile devices at DMC can be revoked at any time.

I understand that violations of these provisions may result in the confiscation of the DMC owned mobile device by the DMC administration, any other designated representative, or local law enforcement and that legal action may be taken.

I agree to be responsible for compensating DMC for any losses, costs or damages incurred due to violations associated with the use of the DMC owned mobile devices.

User Signature _____ Date _____

IT Analyst Signature _____ Date _____