SUNY DOWNSTATE MEDICAL CENTER
Information Services Division
POLICY AND PROCEDURE

No: _____

Subject: Wireless Network Access Policy | **Page** 1 **of** 2

Prepared by: Joel Stern | **Original Issue date:** 11/09/04

Reviewed by: Bert Robles | **Supersedes:** DCC04D

Approval Date: _____

Approved by: Bert Robles, Chief Information Officer | **Distribution:**

Co-Chair Enterprise It Steering Committee: | **Issued by:**

Overview

I. Purpose

The SUNY Downstate Medical Center's (DMC) wireless network is designed to be a convenient supplement to the wired network for general functions including web browsing, email and printing to public printers. Wireless "access points" located in many areas of campus allow approved computers equipped with wireless network cards to make wireless connections to the Internet.

To promote efficient and secure wireless network access, The SUNY Downstate Medical Center's Network Technology Group maintains strict standards for the deployment of wireless devices at DMC.

II. Definition(s): None

Description of Software Application:

Wireless Access Point Policy is different for each area of the Campus.

1) **Residence Halls and Dorms**: The only APs allowed in these areas are the ones set up by NTG and ESC. These access points are attached to the secure wireless VLAN for these buildings. Users attaching via these AP are authenticated by Cisco Clean Access Server and their machines are scanned to insure they meet Downstate Policy **DCC04A.**
2) **Hospital and OPD:** The only wireless network allowed in the Hospital and OPD area is the UHBPHARM network used to control the PYXIS robot. This network does not have access to the Internet or general Downstate Network.

3) **BSB:** Any wireless access point installed in the BSB must be approved by NTG x2593. These access points will only be connected to the secure wireless VLAN for the BSB this VLAN allows access to the Internet and to Library resources. Alternatively WEP can be activated on these APs and they will be allowed on the network till BSB wide wireless network becomes available.

1. **Protected Health Information:** _**X**__Yes ___No

III. Policy:

DMC requires all individuals using information technology devices connected to the DMC network to take appropriate measures to comply with the security of those devices.

IV. Responsibilities (Include all departments/services involved in development/implementation and/or monitoring):

Enforcement: all wireless networks at Downstate must be coordinated through and approved by NTG; any unauthorized wireless access point will be disconnected from the Downstate network and its users will be subject to the sanctions in section VI of the Computer and Network Usage Policy.

VI. Provisions for Testing:

- **NTG will perform periodic scans to determine compliance with this policy**

VII. Reasons for Revision: New Security Software

VIII. Attachments: None

IX. Referenced: HIPAA Regulations

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

* No expectation of Privacy: Messages that are created, sent or received using the UHB email system are the property of UHB. The hospital reserves the right to access and monitor all messages and files on the system. A user's password, any method of encryption, or a user's capacity to delete or purge files or messages, whether authorized by the UHB or not, shall not be understood to give a user any expectation of privacy in any email message.