SUNY DOWNSTATE Medical Center

STAFF CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION STATEMENT

This statement applies to all SUNY Downstate employees, physicians, volunteers, students, trainees, residents, interns, temporary personnel, consultants and contractors.

SUNY Downstate Medical Center is committed to protecting the privacy and confidentiality of health information about its patients while complying fully with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Protected health information is strictly confidential and should never be given, nor confirmed, to anyone who is not authorized under our policies or applicable law, statute, and/or regulation to receive this information.

Definitions:

Protected Health Information (PHI)- Any patient information, including very basic information such as their name or address, that (1) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

Our policies apply to protected health information in any form, including spoken, written or electronic form. It is the responsibility of every hospital staff member and medical staff member to protect the privacy and preserve the confidentiality of all protected health information. This includes, but is not limited to, compliance with the protective procedures below.

1. Public Viewing/Hearing

All SUNY Downstate staff members are required to keep protected health information out of public viewing and hearing. Protected health information should not be left in conference rooms, out on desks or on counters or other areas where the information may be accessible to the public or to other employees who do not have a need to know the protected health information. SUNY Downstate staff members must also refrain from discussing protected health information in public areas, such as elevators and reception areas, unless doing so is necessary to provide treatment to one or more patients. SUNY Downstate staff members must review the patient's record for documented patient restrictions or objections before sharing information with friends and family of the patient.

2. Databases and Workstations

SUNY Downstate staff members are required to exit any confidential database upon leaving their workstations so that protected health information is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. Notepad may not be used to document protected health information, as it is not password protected. SUNY Downstate staff members are *(*also expected) not to disclose or release to other persons any item or process which is used to verify their authority to access or amend protected health information, including but not limited to, any passwords, personal identification numbers, access cards or electronic signature. Staff members will be held responsible and accountable for all activities occurring under his/ her account. These activities may be monitored.

3. Downloading, Copying or Removing

SUNY Downstate staff members are not to download, copy or remove from SUNY Downstate any protected health information, except as necessary to perform their duties. Upon termination of employment or contract with SUNY Downstate, or upon termination of authorization to access protected health information, staff members must return any and all copies of protected health information in their possession or under their control. In addition, staff members must ensure that all protected health information is disposed of in an appropriate manner. Health information in old PC's that are being removed must be deleted.

4. Emailing and Faxing Information

SUNY Downstate staff members are not to transmit protected health information over the Internet (including email) and other unsecured networks unless using a secure encryption procedure. Appropriate policies must be followed when faxing patient information, including using a cover sheet containing a confidentiality notice, ensuring that the fax machine is located in a secure location and verifying receipt with the intended recipient, when appropriate.

5. Curiosity/ Concern/ Personal Gain/ Malice

SUNY Downstate staff members are not to access, review or discuss information for purposes other than their stated duties. Staff members may not look up birth-dates, addresses of friends or relatives or review the record of a public personality. SUNY Downstate staff members are nor to access, review or discuss patient information for personal gain or for malicious intent.

6. Policies & Procedures

SUNY Downstate staff members are required to adhere to all of SUNY Downstate's HIPAA privacy policies and procedures, including campus and department specific policies. All HIPAA Privacy policies can be located at www.downstate.edu/hipaa. The appropriate supervisor should be consulted if a staff member is unsure how to proceed in a specific circumstance.

7. Training

SUNY Downstate staff members are required to complete Downstate's HIPAA training program within two (2) weeks of orientation.

8. Violations

Violators of this policy are subject to employment, civil and criminal penalties. A staff member who has reason to believe that another person has violated SUNY Downstate Policies is to report the matter to his/her immediate supervisor for further action.

I acknowledge that I have received SUNY Downstate Medical Center's Staff Confidentiality of Protected Health Information Statement.

_____	_____	_____
Print Name of Staff Member	Signature of Staff Member	Date