SUNY DOWNSTATE Medical Center

WORKFORCE CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION ATTESTATION

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

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.

SUNY Downstate workforce members should never remove protected health information from Downstate's premises. If protected information must be removed for the performance of your job duties, you are responsible for ensuring that all of the reasonable and appropriate safeguards, including those listed below, are implemented at all times.

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 member of the hospital's workforce and medical staff to protect the privacy and preserve the confidentiality of all protected health information, whether onsite or offsite. This includes implementation of reasonable and appropriate safeguards at all times and compliance with the protective procedures below.

1. Public Viewing/Hearing

All SUNY Downstate workforce 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 workforce members must also refrain from discussing protected health information in public areas, such as elevators and reception areas. Curtains should be drawn in semi-private patient rooms and treatment related discussions should be held in lower tones. SUNY Downstate workforce members must review the patient's record for documented patient restrictions or objections before sharing information with friends and family of the patient, even if the individual is at the patient's bedside.

2. Databases and Workstations

SUNY Downstate workforce 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. Monitors should never be facing a public view. SUNY Downstate workforce members are 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 signatures. Workforce 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 workforce members are not to download, copy or remove from SUNY Downstate any protected health information, except as necessary to perform their duties. All SUNY Downstate faculty and other workforce members are required to encrypt files, documents, and messages containing sensitive or confidential information for protection against unauthorized disclosure while in process, storage or transit. USB drives & portable devices that are not encrypted are only authorized for temporary storage or file sharing between authorized users while the drives/devices are on-site. Drives & portable devices may not be taken off- site without the data either being permanently deleted or encrypted in accordance with SUNY Downstate standards. Long term or permanent storage of SUNY Downstate related files on USB drives and portable devices must meet SUNY Downstate encryption standards. Portable devices include but are not limited to, laptops, notebooks, hand-held computers, tablets (i.e. iPads), Personal Digital Assistants (PDAs), smart phones, and USB drives. Upon termination of employment or contract with SUNY Downstate, or upon termination of authorization to access protected health information, workforce members must return any and all copies of protected health information in their possession or under their control. In addition, workforce members must ensure that all protected health information is disposed of in an appropriate manner, either by shredding or placing the PHI in assigned, secure bins. Health information stored in old PC's that are being removed must be properly and permanently deleted.

4. Emailing and Faxing Information

It is mandatory that only SUNY DMC Lotus Notes email messages be used for confidential communication purposes. Personal email accounts must never be used in the transmission of any PHI. SUNY Downstate workforce members are not to transmit protected health information over the Internet (including email) and other unsecured networks unless using the secure encryption procedure offered via Lotus Notes. 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 workforce members are not to access, review or discuss information for purposes other than their stated duties. Workforce members may not look up birth-dates, addresses of friends or relatives or review the record of a public personality. SUNY Downstate workforce members are not to access, review or discuss patient information for personal gain or for malicious intent.

6. Policies & Procedures

SUNY Downstate workforce 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 workforce member is unsure how to proceed in a specific circumstance.

7. Training

SUNY Downstate workforce 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.

9. Reporting a Violation or Concern

All workforce members must report activities that may involve ethical violations or criminal conduct. Reports can be made to the Compliance Line:

(877) 349-SUNY (7869) – Toll Free, 24-hours-a-day, 7-days-a-week; or

Click on the "Compliance Line" link at www.downstate.edu to make a report via the web.

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