# SUNY DOWNSTATE HEALTH SCIENCES UNIVERSITY

UNIVERSITY HOSPITAL OF BROOKLYN
POLICY AND PROCEDURE

| | | | |
|---|---|---|---|
| | | | **No. HIPAA-23** |
| **Subject:** | **SAFEGUARDS FOR PROTECTED HEALTH INFORMATION** | **Page 1 of 5** | |
| **Prepared by:** | Shoshana Milstein, RHIA, CHP, CCS | **Original Issue Date:** | 12/2002 |
| **Reviewed by:** | Renee Poncet<br>Kevin O'Mara, Esq. | **Supersedes:** | 12/2016 |
| **Committee Approval:** | Executive Performance Improvement Council (EPIC) | **TJC Standards:** | RI.01.01.01: The hospital respects, protects, and promotes patient rights.<br>IM.02.01.01. The hospital protects the privacy of health information.<br>IM.02.01.03: The hospital maintains the security and integrity of health information. |
| | | **Effective Date:** | 9/2019 |
| | | **Issued by:** | Regulatory Affairs |

## I. PURPOSE

SUNY Downstate Health Sciences University will implement appropriate administrative, technical and physical safeguards to ensure that protected health information (PHI) is reasonably safeguarded from intentional or unintentional use or disclosure to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations.

## II. POLICY

This policy establishes the minimum administrative and physical safeguards that must be in place for all designated healthcare components of SUNY Downstate Health Sciences University. Healthcare components may not disclose PHI to other, non-healthcare, components without patient authorization or as permitted by law.

In addition, safeguards must be in place at all times for all uses and disclosures, whether the PHI is on-site or off-site. Where possible, medical record number will be used instead of patient name. Furthermore, on all occasions, minimum necessary guidelines will be followed.

The development of the procedure section is the responsibility of the respective department. It is dependent upon the unique needs of each department's operating structure and shall be advanced and customized accordingly.

## III. DEFINITION(s)

None

## IV. RESPONSIBILITIES

It is the responsibility of all medical staff members and hospital staff members to comply with this policy. Medical staff members include physicians as well as allied health professionals. Hospital staff members include all employees, medical or other students, trainees, residents, interns, volunteers, consultants, contractors and subcontractors at the hospital.

## V. PROCEDURE/GUIDELINES

### A. <u>On- Site versus Off- Site Information</u>

1. Original paper records, medical charts and electronic or paper copies containing PHI should not be removed from Downstate's premises unless absolutely necessary, such as to provide care or treatment to a patient or when required by law.
2. Removal of PHI carries inherent risk. The person removing the PHI is responsible for ensuring the following:
    a. The need for removal meets the applicable criteria;
    b. The contents of the electronic or paper- based PHI is known to the user;
    c. The PHI is secured during its transport;
    d. All appropriate safeguards are implemented to protect the PHI while off-site; and
    e. The PHI is properly returned, in a timely manner, to Downstate.
3. All of the safeguards delineated in Section V.B. through V.D. must be applied to SUNY Downstate's PHI at all times, whether the PHI is on- site or off- site.

### B. <u>Verbal Communications</u>

1. Professional Discussions- SUNY Downstate staff members must refrain from discussing patient information in public areas, such as elevators and cafeterias.
    a. In semi-private rooms, staff members are expected to draw the curtains and talk in low tones.
    b. When PHI must be discussed with a patient in a waiting room, the patient should be taken to an area with less people and spoken to in low tones.
2. Voice Messages
    a. Scripts should be developed for repetitive voice messages, such as appointment reminders, to ensure that no information linking the patient to a particular condition or information about services being provided is indicated. For example, the following message would be appropriate:

    > "This is Paula Green from SUNY Downstate Health Sciences University. I am calling to remind Mrs. Jones of her appointment with Dr. Smith tomorrow at 1:00 PM."

    b. Lab and other test results should never be left in a message.

c. Dictations should not be made within earshot of other individuals.

d. When processing information left on answering machines, the information should not be played over speakerphone.

3. Telephone Requests for Patient Information- The guidelines delineated in the policy Telephone Requests for Patient Information should be followed.
4. Intercom Announcements- Intercom announcements should never reveal the:
   a. Nature of the patient's condition; or
   b. Specialty of services being provided.

   The patient should be referred to the reception desk if protected health information must be disclosed.
5. Patient Family Members & Visitors- When doing rounds or otherwise entering a patient's room to discuss their care, treatment or medications, always be wary of any family members or visitors that are in the room and check with the patient or review his/her chart for consent before initiating such a discussion.

## B. <u>Paper Based Data</u>

1. Sign-In Sheets
   a. Sign-in sheets should never contain PHI, such as the reason for visit, chief complaint or diagnosis. Patient name, date and time would be appropriate elements.
   b. If possible, patients should be given a sticking label to sign-in, where their name, date and time could be documented. The receptionist should then stick the label on the main sign-in sheet maintained by the staff behind the counter. In this manner, the unintended disclosure of the names of the patients who have already signed in will be minimized.
2. Patient Charts
   a. Patient medical records on the nursing floors should be placed in the designated closed trays outside each patient room.
   b. In all other areas, patient charts should be placed in the trays outside the patient rooms with the name of the patient facing the wall.
3. Patient Names on Doors- Patients who have opted out of being included in the facility directory should not have their names posted on the doors.
4. Patient Care Signs/ Logs- This information can continue to be posted as long as access is limited. Examples include:
   a. "High Fall Risk" sign at patient bedside;
   b. "Diabetic Diet" sign at patient bedside;
   c. Use of X-ray lightboard at nursing station; or
   d. Use of Inpatient logs at nursing station.
5. Securing PHI Before Leaving
   a. SUNY Downstate staff members are expected to place any PHI in closed drawers before going on breaks, to lunch and at the close of business each day.
   b. Information should not be left in conference rooms or on counters where the information may be accessible to the public.
   c. Any PHI removed from DMC premises must not be left unattended in places where unauthorized persons can gain access, legally or otherwise.
6. Postcards- Postcards sent to patients should not contain any PHI.
7. Interoffice Mail
   a. Reasonable safeguards should be taken to ensure the confidentiality of PHI during delivery.

   b. Such safeguards may include personally delivering the information, sealing the envelope or marking it as confidential.

8. Closets & Cabinets- All closets and cabinets containing PHI and confidential files must be locked when the area is unsupervised and access must be monitored.
9. Transporting PHI- PHI should be placed in bags or envelopes that are made inaccessible for viewing by the transporter.
10. Destruction of PHI / Shredding- All printed materials and copies, including faxes, emails and reports, containing PHI, including even just a patient's name, must either be shredded or placed in secure bins designated for shredding. Under no circumstances may this information be placed in regular trash bins.
11. Faxing- The guidelines delineated in the policy Faxing Patient Information should be followed.

### C. <u>Electronic Data</u>

1. Computer Terminals
   a. PC monitors should be turned away from the public.
   b. For those PC's that are located in high traffic areas that cannot be moved to another location, shields should be placed on the monitors.
   c. SUNY Downstate staff members are expected to log off of terminals before leaving their workstations.
   d. Passwords and ID's cannot be shared. Staff will be held liable for all activity occurring under their account.
   e. The department supervisor is responsible for ensuring that old PC's that are being removed are referred to Information Services so that any protected health information is deleted / destroyed appropriately.
2. Diskettes & CD's- PHI on diskettes or CD's must be deleted or destroyed. SUNY Downstate department supervisors are responsible for inspecting the diskettes or CD's for any valuable necessary information and then breaking the diskette film, cutting the CD or placing these electronic materials in secure bins designated for shredding.
3. Emails- It is mandatory that only SUNY Downstate's Email System email messages be used for any and all PHI communications. Personal email accounts must never be used for the transmission of any PHI. Any PHI being transmitted over the internet (including email) must be encrypted.
4. USB Drives/ Portable Devices- USB drives and portable devices (including, but not limited to, laptops, notebooks, hand-held computers, tablets, personal digital assistants, smart phones, and USB drives) that are not encrypted are only authorized for the temporary storage or file sharing between authorized users while the device / drives are on-site. Portable devices may not be taken off- site without the data either being permanently deleted or encrypted in accordance with DMC encryption standards. Long term or permanent storage on a portable device must meet encryption standards.
5. Use of Social Media Sites- PHI must not be posted on social media sites including Facebook, Instagram or Twitter.
6. Role Change / Termination- The applicable role change or termination procedures must be followed to ensure electronic access to PHI is discontinued when appropriate.

### D. <u>Physical Security</u>

1. Ample Space
   a. Ample space should be provided to discuss information with patients and other providers, to answer telephone calls and to conduct other operations involving PHI.
   b. When ample space cannot be provided, physical barriers should be erected to decrease sound penetration (Ex: cubicle walls, dividers, shields, potted plants).
2. Key / ID Badge Distribution
   a. Distribution of keys to areas containing PHI must be supervised and controlled.
   b. Keys, access cards and tokens may not be shared.
   c. Upon termination, all keys and badges must be returned.
3. Locked Doors- Doors must be locked and access to sensitive work areas must be monitored.

4. Escorting Visitors and Patients- Visitors and patients must be appropriately escorted or monitored in areas where PHI is located to ensure that they do not have access to PHI regarding other patients.

   Persons including, but not limited to, pharmaceutical representatives and device salesmen who are not employed by DMC, shall not be in areas in which patients are being seen or treated, or where PHI is stored, without appropriate supervision.

### E. Reporting a Violation

All workforce members must report activities that may involve ethical violations, concerns or criminal conduct, including suspected violations of this policy or the theft or loss of any PHI. 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.

## VI. ATTACHMENTS

None

## VII. REFERENCES

Standards for Privacy of Individually Identifiable Health Information, 45 CFR §164.530(c)

| Date Reviewed | Revision Required (Circle One) | | Responsible Staff Name and Title |
|---|---|---|---|
| 9/2013 | (Yes) | No | Shoshana Milstein, AVP, Compliance & Audit |
| 9/2016 | (Yes) | No | Shoshana Milstein, AVP, Compliance & Audit |
| 12/2016 | Yes | (No) | Shoshana Milstein, AVP, Compliance & Audit |
| 9/2019 | Yes | (No) | Alexandra Bliss, Compliance Coordinator |