SUNY Downstate Medical Center

HIPAA

POLICY

&

PROCEDURE

GUIDE

FRONT END AREAS

Office of Compliance & Audit Services

Table of Contents

I. Notice of Privacy Practices: Page 3

II. Disclosing Downstate Directory Information: Page 6

III. Additional Patient Privacy Rights: Page 7

IV. Disclosures of Patient Information: Page 9

V. Safeguarding Patient Information: Page 12

NOTE: THE INFORMATION CONTAINED IN THIS GUIDE PRESENT ONLY A SUMMARY OF THE SPECIFIED POLICIES. THE COMPLETE POLICIES AND ASSOCIATED FORMS ARE LOCATED IN THE UHB ADMINSTRATIVE POLICY & PROCEDURE MANUAL. THEY CAN ALSO BE VIEWED AND DOWNLOADED FROM DOWNSTATE'S HIPAA WEBSITE AT www.downstate.edu/hipaa. SELECT THE LINK FOR "SUNY DOWNSTATE HIPAA PRIVACY POLICIES", THEN "OPD, ADMITTING & REGISTRATION".

I. Notice of Privacy Practices

For complete policy, see "Notice of Privacy Practices".

A. SUNY Downstate's Notice of Privacy (NOP) describes how our patients' medical information may be used and disclosed and how patients can get access to their information.

1. The NOP describes the health information privacy practices of SUNY Downstate Medical Center, its medical staff and affiliated healthcare providers that jointly provide healthcare services with Downstate.

2. The NOP includes information regarding the following:

   a. Requirements for a patient's written authorization before using or disclosing health information;
   b. Situations which do not require a patient's authorization before the health information is disclosed;
   c. The patient's right to inspect and copy health information;
   d. The patient's right to amend health information that is believed to be inaccurate or incomplete;
   e. The patient's right to an accounting of disclosures which identifies individuals to whom Downstate has disclosed health information;
   f. The patient's right to request further restrictions on the way Downstate uses the health information, as well as to request a confidential method of contact;
   g. The patient's right to name a personal representative who may control the privacy of the health information.

B. Provision of the NOP

1. The registrars must provide a NOP to each patient, the first time they receive care from SUNY Downstate.

   a. If the first service is delivered to a patient electronically or via the telephone, the notice must be automatically provided electronically.
   b. A patient who received an electronic notice may obtain a paper copy, upon request.

2. The NOP is available in English, Spanish and Creole. For other language interpretation, the registrar should contact Patient Relations.

3. In addition to the general NOP, a specific NOP should be provided to patients with the following diagnoses:

a. For an HIV diagnosis, provide the NOP on “Confidentiality of HIV-Related Information”;
b. For alcohol/ drug abuse, provide the NOP on “Confidentiality of Alcohol & Drug Abuse Information and HIV- Related Information”;
c. For mental illness, provide the NOP on “Confidentiality of Mental Health Information and Psychotherapy Notes”.

4. In an emergency situation, the NOP must be provided as soon as reasonably practicable after the emergency treatment.

5. The registrar must obtain the patient’s written acknowledgement of receipt of the NOP on the HIPAA Privacy Form.

   a. If the patient refuses to sign, the registrar should document his/her good faith efforts to obtain patient acknowledgement and the reason for the patient’s refusal.
   b. The HIPAA Privacy Form must be placed in the patient’s medical record.

C. Entry of NOP into Eagle System

1. When the patient is provided the first service, the Eagle system must be updated to reflect the provision of the NOP to the patient.

2. The information should be entered into two fields in the Patient Master Maintenance (PMM) screen:

   a. **N-O-P DT** field: Enter the date the NOP was provided in MM/DD/YYYY format;
   b. **N-O-P** field: The following options are available for this field:
      i. “**A**”: Received acknowledgement from patient;
      ii. “**C**”: Child- NOP given to parent;
      iii. “**E**”: Emergency- to be given after emergency treatment;
      iv. “**L**”: Lookup only- patient not being seen;
      v. “**P**”: Pre-registration only;
      vi. “**R**”: Patient refused acknowledgement.

3. The following guidelines should be followed when entering information into the “N-O-P” field:

   a. “A” should be selected when the notice was given to the patient and the patient acknowledged receipt on the HIPAA Privacy Form;
   b. “C” should be selected when the patient is a minor/ child and the notice was given to the parent or guardian;
   c. “E” should be selected when the patient is in an emergency situation and cannot receive the notice of privacy. Once the

emergency treatment is over and a NOP has been provided to the patient, registrars must update this field with an “A” for receiving the notice and acknowledging receipt or a “R” for receiving the notice and refusing to acknowledge;

d. “L” should be selected when the record is being accessed for a lookup of information only and the patient is not currently being seen;
e. “P” should be selected when the patient is only being pre-registered for a visit or admission;
f. “R” should be selected when the notice was given to the patient and the patient refused to acknowledge receipt.

4. For each registration or admission, the registrar must review the N-O-P field to ensure that the notice has been provided to the patient and documented in Eagle. The field should be updated in the following situations:

   a. If the field reflects an “E”, the previous visit was an emergency situation, so the patient may not have received the notice;
   b. If the field reflects a “L”, the patient’s record was only accessed to lookup information. The patient needs to receive a notice;
   c. If the field reflects a “P”, the patient was only pre-registered and could not have received a notice.

II. Disclosing Downstate Directory Information

For complete policy, see "Facility Directory".

A. The following information is considered, under HIPAA, to be "facility directory" information:

1. Patient Name;
2. Location (including room # and telephone #);
3. General Condition (poor, good, critical);
4. Religious Affiliation.

B. The patient's room location, telephone number and general condition (no diagnosis) may be disclosed to any individual who requests about a patient by name. The patient's religious affiliation may be disclosed to clergy.

C. The patient has a right to opt out of being included in the facility directory.

1. The staff member must provide the "Facility Directory" form to the patient who requests to opt out of the directory.

2. The completed form should be placed in the front of the patient's medical record.

3. The opt out request must then be entered into the Eagle system:

   a. For patient admissions, on the **"Admission Maintenance"** screen, the staff member must enter **"N"** in the **"Release"** field;
   b. For clinic visits, on the **"Clinic Visit Maintenance (1-REG)"** screen, the staff member must enter **"N"** in the **"Release"** field.

4. Upon receiving a request for facility directory information, including admit and discharge dates, the staff member must perform the following:

   a. Review the patient's medical record for the Facility Directory form. If the form is present, the staff member must abide by the patient's opt out request and ensure that no information is disclosed; and
   b. Review the **"Front Desk Inquiry"** (FDI) screen in the Eagle system to determine if the patient has opted out. If either the "Latest Inpatient Admission Information" or the "Latest Outpatient Information" is blanked out and the screen states "CONFIDENTIAL", the patient has opted out and the facility directory information, including admit and discharge dates, may NOT be disclosed.

III. Additional Patient Privacy Rights

For complete policy, see:
"Uses & Disclosures for Individuals Involved in Care & for Notification Purposes";
"Patient Requests for Additional Privacy Protections".

A. Patients should be given the opportunity to identify a family member or friend to be involved in the patient's care and for notification of the patient's location, general condition or death.

   a. When the patient signs the Notice of Privacy acknowledgement on the HIPAA Privacy Form, the patient should be advised to complete Section II of the form, specifying the family member/ friend who is authorized to be involved in the patient's care.

   b. This individual should then be entered into the Eagle system:
      i. Select **"RFP"** for Related Party Maintenance;
      ii. Select **"1"** for R/P, Related Parties;
      iii. Enter the individual's name, relation, address and phone number;
      iv. In the **"DIS CARE"** field, enter **"Y"** (this identifies the individual as someone whom the patient allows Downstate to discuss his/her care);
      v. The face sheet with the identified related party information should be printed and filed in the medical record.

B. Patients have a right to request that Downstate restrict the way it uses and discloses their PHI for treatment, payment or healthcare operation purposes or that Downstate communicate with them in a method or location that is more confidential to them (including communications for mailings and appointment reminder calls).

   1. The patient must complete the "Request for Additional Privacy Protection" form.

   2. The registrar should then contact Patient Relations to review the request and to determine whether the restriction should be granted or denied.

   3. Patient Relations will notify the patient via the "Notice of Additional Privacy Protection Request Review" form.

   4. If the request was approved, the Notice of Additional Privacy Protection Request Review form should be placed in the front of the medical record and all hospital staff involved in the patient's care must be notified of the restriction or confidential communication request.

5. In addition, a request for confidential communications must be entered into the Eagle system. The staff member should perform the following steps:

    a. Select **"RPF"** for Related Party Maintenance;
    b. Select **"4"** for **"TAD- Temp Address"**;
    c. On the following screen, enter **"PMF"** in the **"LINK"** field;
    d. If the patient has specified an alternate address, enter the address in the **"ADDR-1"** field; if none has been specified, enter **"N/A"** in the field;
    e. In the **"ADDR TYPE"** field, enter **"P"** for Privacy Request-Alternate Communication;
    f. If the patient has specified an alternate phone number, enter the number in the **"PHONE/HOME"** field;
    g. In the **"REMARKS"** field, enter any specific request the patient may have made;
    h. If the patient has requested that this alternate communication should be used for only a certain period of time, enter in the specific dates in the **"START DATE"** and **"UNTIL DATE"** fields;
    i. Hit <enter> to update the information.

6. The restriction/ confidential communication may be modified or terminated. The "Modification/ Termination of Restriction" form should be provided to the patient. The completed form should be placed in the medical record and the Eagle system should be updated to reflect the modification.

C. The registrar should refer the patient to the Health Information Management (HIM) Department for the following requests:

1. Requests to inspect medical records;
2. Requests for copies of medical records;
3. Requests for summaries/ explanations of medical records;
4. Requests for amendment of medical records;
5. Requests for an accounting of disclosures.

IV. Disclosures of Patient Information

For complete policy, see:
"Uses & Disclosures for Treatment, Payment and Healthcare Operations";
"Uses & Disclosures Not Requiring Patient Authorization";
"Uses & Disclosures of Decedent Information";
"Uses & Disclosures Requiring Patient Authorization";
"Accounting of Disclosures";
"Personal Representatives";
"Privacy Rights of Minors";
"Minimum Necessary Guidelines".

A. Any requests for patient information that is necessary for treatment, payment and healthcare operations do NOT require a patient authorization. If these requests provide a patient's authorization, the form does not need to meet the HIPAA requirements.

   1. Treatment includes requests from other providers or healthcare organizations in order to continue the care of the patient.
   2. Payment includes requests for billing, utilization review and claims management.
   3. Healthcare operations include operational and administrative activities such as quality assessment, credentialing, legal review and business management.

B. There are additional circumstances where patient information may be disclosed without obtaining the patient's authorization. In unclear circumstances, contact the HIM department to determine whether the requested information can be disclosed.

   1. Disclosures required by law may be released. Subpoenas should be sent to the HIM department for its review of appropriate documentation.

   2. Public health activities do not require patient authorization:

      a. To prevent or control a disease- including reporting diseases, injuries, births, deaths to state agencies and conducting public health surveillance;
      b. To report child abuse or neglect;
      c. To the FDA to monitor the safety/ effectiveness of a product;
      d. To control a communicable disease.

   3. Health oversight agencies, such as the NYC Department of Health, do not require patient authorization.

4. Under certain conditions, PHI may be disclosed to law enforcement officials and for specialized government functions. Risk Management and the Attending Physician should be contacted.

5. PHI regarding decedents may be disclosed to coroners, medical examiners and funeral directors in order to carry out their duties.

6. Organ procurement organizations may receive information in order to facilitate donation and transplantation.

C. The above disclosures of information that can be made without patient authorization must be documented so that an accounting of disclosures can be provided to the patient, when requested.

1. Examples of disclosures that must be documented include:

   a. NYC Department of Health reviews/ audits;
   b. JCAHO reviews;
   c. Vital statistics reports sent to state agencies.

2. The department should send a copy of the PHI request (ex: DOH or JCAHO letter, birth/ death reports) to the HIM department for inclusion of the disclosure in its accounting of disclosures database.

3. In addition, the department should maintain the following information for each patient information disclosure:

   a. Date of disclosure;
   b. Name of person/ organization receiving PHI;
   c. Address of person/ organization receiving PHI (if known);
   d. Brief description of PHI disclosed;
   e. Brief statement to the purpose of the disclosure- a copy of the written request may be used in lieu of a statement.

D. All other requests for PHI require a patient's authorization and should be referred to the HIM department.

E. Under NYS law, the following individuals qualify as a "personal representative" and can authorize the use/ disclosure of a patient's PHI.

1. Healthcare proxy or agent- The agent's authority begins when a determination has been made that the patient lacks capacity to make healthcare decisions.

2. Parent/ guardian of a minor (<18 years of age)- In the following circumstances, the minor retains control over his/ her PHI; however, the attending physician should make the final determination:

    a. Emancipated minor- a minor who is married or has children;
    b. When the minor can lawfully obtain services without parental consent, such as for treatment of a sexually transmitted disease, for abortion or for prenatal care of a pregnant minor;
    c. When the parent has agreed to a confidential relationship with the minor and the provider; or
    d. Where the minor obtains care at the direction of the court.

3. Guardian/ committee appointed for an incompetent individual, pursuant to the Mental Hygiene Law.

4. A distributee of a deceased subject for whom no personal representative exists- The following documentation must be provided:

    a. A certified copy of the patient's death certificate;
    b. A notarized affidavit containing the following or similar attestation: "I am a distributee of the named decedent's estate as the term 'distributee' is used in §18 of the New York Public Health Law and defined by §1-2.5 of the New York Estates, Powers and Trusts Law and no 'personal representative' as that term is defined by §1-2.13 of the New York Estates, Powers and Trusts Law, has been appointed for the deceased subject named herein."

5. Attorney who holds a power of attorney from a qualified person or from the patient's estate- The following must be provided:

    a. A copy of the power of attorney that explicitly authorizes the attorney to request access to patient information;
    b. Access to PHI must be subject to the duration and terms of the power of attorney.

F. All requests for PHI must be limited to the minimum amount of information that is reasonably necessary to achieve the intended purpose or activity.

1. A form should be used to document the information requested and the minimum information provided. The form should be filed in the medical record.
2. For routine uses and disclosures, the Departmental Manual should specify the minimum information necessary in each circumstance.

V. Safeguarding Protected Health Information

For complete policy, see:
"Safeguards for Incidental Disclosures";
"Verification of Identity";
"Telephone Requests for Patient Information";
"Faxing Patient Information";
"Staff Confidentiality".

A. Protected Health Information (PHI) must be reasonably safeguarded from intentional or unintentional use or disclosure.

1. Verbal communications

    a. Patient information should not be discussed in public areas, such as elevators and cafeterias.
    b. In semi- private rooms, staff should draw the curtains and talk in low tones.
    c. In waiting rooms, the patient should be taken to an area with less people and spoken to in low tones.
    d. Voice messages and intercom announcements should never reveal a specific condition or the particular services being provided.

2. Paper based information

    a. Sign- in sheets should never contain PHI, such as the reason for the visit, chief complaint or diagnosis.
    b. Patient charts on the nursing floors should be placed in designated closed trays outside each patient room.
    c. In the outpatient areas, the charts should be placed facing the wall so that the patient's name cannot be determined.
    d. Patient information should not be left in conference rooms or on desks where the information may be accessible to the public.
    e. Cabinets containing PHI must be locked when the area is unsupervised.
    f. PHI should be placed in envelopes when transporting.
    g. All PHI must be shredded.

3. Electronic information

    a. Computer monitors should be turned away from the public or should have privacy shields.
    b. Staff members must log off of their computers before leaving their workstations.
    c. Passwords and ID's cannot be shared.

d. Disks or CD's that contain PHI must be shredded.
e. Emails containing PHI should be encrypted.

B. Staff members are required to verify the identity and authority of unknown individuals requesting access to PHI. The HIM department should be contacted for medical record requests.

1. Patients must present a photo ID.
2. Personal representatives must present a photo ID and documentation of their authority over the patient (see "Requests for Patient Information").
3. Public officials must present an agency identification badge or a written request on appropriate agency letterhead.

C. PHI may be disclosed over the telephone if it is necessary for the immediate needs of patient care, if a loss of reimbursement can result or during system downtime when information cannot be accessed via the computer systems.

1. For unknown internal requests, the caller should be directed to the nearest workstation.
2. For unknown external calls, the request should be faxed on official agency letterhead. For patient requests, the fax should document the patient's signature or the personal representative's authority over the patient.
3. Sensitive information should never be disclosed via the telephone.

D. PHI may be faxed if it is necessary for the immediate needs of patient care, if a loss of reimbursement can result or during system downtime when information cannot be accessed via the computer systems.

1. Faxes containing PHI must utilize Downstate's standard "Facsimile Cover Page".
2. Staff members should make reasonable efforts to ensure that the fax was transmitted to the correct destination. This includes:

   a. Notifying the receiving party of the fax;
   b. Printing a confirmation from the fax machine;
   c. Auditing pre-programmed numbers to ensure they are accurate and current.

3. Fax machines should be located in secure areas.
4. Incoming faxes should be distributed to the proper recipient expeditiously.
5. Sensitive information may never be faxed.

E. All staff members are required to sign an annual confidentiality statement.

1. All suspected breaches must be reported to the appropriate supervisor, to the Office of Labor Relations or to the Confidential Compliance Hotline at **877-349-SUNY**.
2. Depending upon the severity of the violation, appropriate disciplinary measures will be applied.
3. There will be no retaliation against any staff member who reports a HIPAA Privacy violation.