
# HIPAA

# POLICY

# &

# PROCEDURE

# GUIDE

## HEALTH INFORMATION MANAGEMENT DEPARTMENT

***Office of Compliance & Audit Services***

## Table of Contents



**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 "HEALTH INFORMATION MANAGEMENT/ MEDICAL RECORDS".**

## I. Patient Requests for Medical Records

*For complete policy, see:*
*"Patient Requests for Access";*
*"Designated Record Sets".*

A. Patients have a right to access their Protected Health Information (PHI), including medical records, billing records and research records.

1. Patients must complete the "Patient Request for Access to Health Information" form.
2. For records not maintained in HIM, the HIM staff should send the request to the relevant department (Ex: Radiology, Private Practice).

B. Patients can request copies of their medical records to be picked up or to be delivered by mail.

1. HIM must respond to requests within 30 days for on-site records and within 60 days for off-site records. If there are unusual difficulties, an extension of 30 days may be granted with notification to the patient. See "Extension Notification" form.
2. Patients are entitled to request an explanation or a summary of the PHI maintained in their medical records. The attending physician should be contacted and the explanation/ summary should be added to the patient's medical record.
3. There is a charge for copies of medical records and for the preparation of any explanations or summaries:
   a. $0.75/ per page for patient or personal representatives;
   b. $1.00/ per page for attorneys or insurers;
   c. The charge for explanations/ summaries depends on the number of hours required for the preparation of such documents;
   d. There is no charge for requests to send records to another healthcare provider;
   e. The "Fee Estimate" form should be sent to the patient to inform him/her of the charges for the medical record copies.

C. Patients can request to inspect their records.

1. An appointment should be made for the patient to review his/her records in the HIM department. HIM should ask the patient as to whether or not the attending physician should be present during the review.
2. The patient must provide appropriate identification.
3. A HIM staff member must be present at all times during the review.

D. Under certain circumstances, the patient may be denied access to his/her PHI. For example, correspondence records in the back of the patient's medical record or information disclosed to the provider in confidence by another person on the condition that it would never be disclosed are not required to be released to the patient. (See policy for complete listing of circumstances for denial of access.)

1. Appropriate staff must indicate the grounds for the denial and send the "Notice of Denial" letter to the patient.
2. The patient may appeal the decision and ask for the request to be reviewed by the Medical Records Committee. A "Notice of Denial Review" letter should be sent to the patient within 10 days.
3. If the patient's access is still denied, the patient is entitled to have the request reviewed by a committee appointed by the State of New York and then to the court system for judicial review.

## II. Other Requests for Medical Records

*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";*
*"Personal Representatives";*
*"Privacy Rights of Minors";*
*"Uses & Disclosures for Research Purposes";*
*"Minimum Necessary Guidelines".*

A. Any requests 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 a patient's authorization is not required in order to disclose the PHI.

   1. Disclosures required by law may be released.

      a. Subpoenas must be so-ordered by the court;
      b. Only the information authorized by the order should be disclosed.

   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. All other requests for PHI require a patient's authorization.

1. In order for the request to be honored, it must include the patient's authorization on Downstate's HIPAA Authorization form.

    a. Requests that provide a different HIPAA Authorization form must be returned to the requestor. A copy of Downstate's form should be provided, as well as instructions to the requestor to ensure the completion of Downstate's form.
    b. If the PHI relates to HIV, mental health or alcohol/ substance abuse information, the authorization must explicitly state the information the patient authorizes to be disclosed.
    c. The authorization form must be completed in its entirety, signed and dated. Defective authorizations should be returned to the requestor with an explanation as to why it cannot be honored.
    d. The signed authorization should be filed in the patient's medical record.

2. An authorization form may be revoked.

    a. Upon receipt of a letter of revocation, HIM staff should notify the appropriate personnel to no longer use or disclose the PHI as stated in the authorization.
    b. The letter of revocation should be filed in the medical record, adjacent to the original authorization.

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

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

i. Emancipated minor- a minor who is married or has children;
ii. 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;
iii. When the parent has agreed to a confidential relationship with the minor and the provider; or
iv. Where the minor obtains care at the direction of the court.

c. Guardian/ committee appointed for an incompetent individual, pursuant to the Mental Hygiene Law.
d. A distributee of a deceased subject for whom no personal representative exists- The following documentation must be provided:
   i. A certified copy of the patient's death certificate;
   ii. 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."
e. Attorney who holds a power of attorney from a qualified person or from the patient's estate- The following must be provided:
   i. A copy of the power of attorney that explicitly authorizes the attorney to request access to patient information;
   ii. Access to PHI must be subject to the duration and terms of the power of attorney.

D. Physicians or other providers who request access to medical records for studies must complete the "Medical Record- Provider Study" form. The purpose of the review must be documented. For research studies, the following documentation must be provided:

1. For studies with an IRB approved protocol, the IRB # must be documented on the Medical Record- Provider Study form.
2. For studies preparatory to research, the provider must complete the "Researcher Certification for Review Preparatory to Research" form and append it to the study request.
3. For studies on decedents, the provider must complete the "Researcher Certification for Review on Decedents" form and append it to the study request.
4. For studies with an IRB approved waiver of authorization, the "HIPAA Waiver of Authorization" form must be appended to the study request.

5. For all other research studies, patient authorization is required before the PHI can be disclosed.

E. 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. The “Screening 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 HIM Departmental Manual should specify the minimum information necessary in each circumstance.

## III. Maintaining an Accounting of Medical Record Disclosures

*For complete policy, see "Accounting of Disclosures".*

A. All disclosures of a patient's PHI must be documented so that an accounting of disclosures can be provided to the patient, when requested.

B. The following disclosures lists some disclosures that do not require documentation:

1. Requests for treatment, payment and healthcare operation purposes;
2. Requests with a patient authorization;
3. Disclosures of patient directory information (admit or discharge dates).

C. The following lists some disclosures that must be documented for an accounting of disclosures:

1. NYC Department of Health reviews/ audits;
2. JCAHO reviews;
3. Reports sent to state agencies- such as congenital malformations, terminations of pregnancy, Alzheimer's disease, vital statistics;
4. Provider studies for research purposes.

D. The following information must be documented for each disclosure (See policy for the circumstances under which abbreviated information may be documented):

1. Date of disclosure;
2. Name of person/ organization receiving PHI;
3. Address of person/ organization receiving PHI (if known);
4. Brief description of PHI disclosed;
5. Brief statement to the purpose of the disclosure- a copy of the written request may be used in lieu of a statement.

E. Patients who request an accounting must complete the "Patient Request for Accounting of Disclosures" form.

1. HIM staff must respond within 60 days. An extension of 30 days may be provided with notification to the patient. The "Extension Notification" form should be utilized.
2. The patient may request an accounting for a period of 6 years. An accounting cannot be provided for disclosures before April 14, 2003.
3. The patient is entitled to one free accounting per 12- month period. If an additional accounting is requested, the "Accounting of Disclosures- Fee Estimate" should be sent to the patient with the estimated charge.
4. All accounting of disclosure requests and communications should be filed in the patient's medical record.

## IV. Disclosing Downstate Directory Information

*For complete policy, see:*
*"Facility Directory";*
*"Uses & Disclosures to Individuals Involved in Care & for Notification Purposes".*

A. The following information is maintained in the facility directory:

1. Patient Name;
2. Location;
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. This also includes admit and discharge dates. 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 restriction will be entered into the Eagle system by the registration staff and a "Facility Directory" form will be placed in the medical record.
2. Upon receiving a request for facility directory information, HIM staff should check the FDI (Front Desk Inquiry) screen in the Eagle system.
3. If the patient has opted out, the facility directory information, including admit and discharge dates, may NOT be disclosed.

D. Disclosure of PHI to family members or friends involved in the patient's care and for notification purposes, in addition to the information contained in the facility directory, must comply with certain requirements. The attending physician should be contacted.

## V. Additional Patient Rights

*For complete policy, see:*
*"Patient Requests for Amendment";*
*"Patient Requests for Additional Privacy Protection".*

A. Patients have a right to amend their health information.

1. Patients must complete "Patient Request for Amendment of Health Information" form.
2. HIM staff should contact Risk Management and the attending physician to determine whether the request should be granted or denied.
3. A response is required within 60 days from the date the request was received. A one time extension of 30 days may be granted under extenuating circumstances. The patient should be notified via the "Extension Notification" form.

B. If the attending physician determines that the amendment is appropriate and the current information is incomplete or inaccurate without the patient's requested amendment, the amendment should be made in the patient's record.

1. The "Notice of Approval of Amendment" form should be sent to the patient.
2. Permission should be requested from the patient to notify all others who have relied upon the original information in a way that would negatively affect the patient.
3. Standard medical record procedures should be followed when making an amendment to a patient's record.
4. Any future disclosures of the amended PHI must include the amended information or a link to the amended information.

C. The attending physician may deny a patient's request to amend his/ her health information.

1. HIM staff should send the "Notice of Denial Letter" to the patient, indicating the grounds for the denial.
2. The patient may submit a statement of disagreement, limited to two pages.
3. The attending physician, in conjunction with HIM, may prepare a rebuttal statement, if necessary to clarify Downstate's position. A copy of the rebuttal must be provided to the patient.
4. The following documents must be included in any future disclosures of the patient's information:

a. Patient's written amendment request;
b. Downstate's Notice of Denial;
c. Patient's statement of disagreement (if any);
d. Downstate's rebuttal statement (if any).

D. Patients also 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..

1. The patient must complete the "Request for Additional Privacy Protection" form.
2. Patient Relations should determine whether the request should be granted or denied.
3. The patient should be notified of the decision via the "Notice of Additional Privacy Protection Request Review" form.
4. If the request was approved, the form should be placed in the front of the medical record and the Eagle system should be updated. All hospital staff involved in the patient's care must be notified of the restriction or confidential communication request.
5. The restriction/ confidential communication may be modified or terminated. The "Modification/ Termination of Restriction" form should be utilized and placed in the medical record.

## VI. Safeguarding Protected Health Information

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

A. 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. Internal emails containing PHI should be encrypted.

B. HIM staff should review requests to determine whether de-identified information can be used (Ex: Student training, research studies).

1. De-identified information is not subject to the HIPAA Privacy standards.
2. It includes removing a list of 19 identifying elements, including:

a. Name, Phone/ Fax #, Email address;
b. Medical record #, Social Security #, Account #;
c. All geographic subdivisions smaller than a State (including street address, city, county, precinct), except for the first three digits of the zip code;
d. All elements of date, including date of birth, admission and discharge dates, dates in progress notes.

C. Staff members are required to verify the identity and authority of unknown individuals requesting access to PHI.

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

D. 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.

E. 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.

F. 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.