HIPAA

POCKET

GUIDE

REVISED 2005

HIPAA Privacy Policies & Procedures
Table of Contents

NOTE: The information contained in this guide present only a summary of the policies specified above. The complete policies and associated forms can be viewed and downloaded from Downstate's website at www.downstate.edu/hipaa. Select the link for "SUNY Downstate HIPAA Privacy Policies" or "UPB/ CPMP HIPAA Privacy Policies".

HIPAA Contacts

- **Privacy Rule**

This rule applies to all Protected Health Information (PHI) maintained in any format, oral, paper or electronic.

Questions/ Complaints:
Office of Compliance & Audit Services
(718) 270-2095
Confidential Hotline: 877-349-SUNY

- **Security Rule**

This rule requires administrative, physical and technical safeguards to protect PHI maintained in an electronic format.

Questions/ Complaints:
Department of Information Services
(718) 270-2431

- **Transaction & Code Sets**

This rule standardized the content and format of electronic healthcare transactions.

Questions/ Complaints:
Hospital Finance
(718) 270-4901

I. Clinical Policies

A. Accounting of Disclosures

- Describes to patient all disclosures made of his/ her PHI without the patient's knowledge.
- Examples include disclosures made for state required reports (ie; vital events, lab testing, tumor registry), disclosures to DOH during an audit and disclosures to JCAHO during an accreditation survey.
- Every department that discloses PHI must have a process or system to document each disclosure, except:
  - ✓ Disclosure made for treatment, payment purposes or for healthcare operations;
  - ✓ Disclosures pursuant to patient authorization;
  - ✓ Facility directory disclosures;
  - ✓ Disclosures to individuals involved in the patient's care;
  - ✓ Incidental disclosures (ex: An overheard conversation).
- The following information must be documented for each disclosure:
  - ✓ Date of disclosure;
  - ✓ Name of organization receiving PHI;
  - ✓ Address of organization receiving PHI;
  - ✓ Brief description of PHI disclosed, including dates of treatment; and
  - ✓ Statement of purpose of disclosure.
- Requests for a patient accounting of disclosures should be directed to the Health Information Management Department.

B. De-Identification of Information

- Whenever possible (such as during conferences or when writing reports), de-identified information should be used.
- De-identified information consists of removing a list of 18 specified items, including:
  - ✓ Name, phone number, email address;
  - ✓ Geographic subdivisions- street, county, city, zip code (except for first 3 digits);
  - ✓ Social security # or medical record #;
  - ✓ All elements of date- DOB, admit date, discharge date;
  - ✓ Biometric identifier or photographic images;
  - ✓ Any other unique code or number.
- See policy on Downstate website for complete listing of identifying elements.
- De-identified information is not subject to HIPAA.

C. Facility Directory

- The following information can be disclosed to anyone asking about the patient by name or to clergy, unless the patient has "opted out" of the directory:
  - ✓ Patient Name;
  - ✓ Location in Hospital;
  - ✓ General Condition (Ex: Fair, critical);
  - ✓ Religious Affiliation (to clergy only).

- Upon admission or registration, the patient can opt out/ restrict the information disclosed in the directory.
- Restriction is entered into University Hospital of Brooklyn's (UHB) Eagle system and information is blocked out on the Front Desk Inquiry (FDI) screen.
- Information is also documented on the Facility Directory form which is placed in the medical record and is used to notify Nursing not to post the patient's name on the outside of his/her room.
- Staff members receiving calls regarding a specific patient should direct the call to Admitting or Registration areas.

D. Faxing Patient Information

- Permitted when original record would not meet the immediate needs of patient care or for reimbursement purposes.
- Sensitive information should never be faxed.
- Must use Downstate Fax Cover Page, available on Downstate HIPAA website.
- When possible, staff should call to inform receiver of the time fax is being sent, as well as ensure that sent fax was actually received.
- Fax machines should be located in secure areas, away from main thoroughfares.

- Received faxes should not be left sitting on fax machines and should be distributed expeditiously.
- Pre-programmed numbers should be audited periodically to ensure numbers are still current and receivers are authorized to receive such information.

E. Minimum Necessary Guidelines

- Staff members must make reasonable efforts to limited permitted uses and disclosures of PHI to the minimum necessary for the accomplishment of the intended function or activity.
- Each department must document the minimum information necessary for each routine use, disclosure and request.
- For non-routine requests, determine the following:
  - ✓ What is the purpose?
  - ✓ What type of information is needed to accomplish this purpose?
  - ✓ What information is likely to be attached and is this information also needed to accomplish the purpose?
- Disclosing an entire medical record needs specific justification. An appropriate justification would be that the disclosure is necessary for the treatment of the patient or for appropriate training of medical students.

F. Notice of Privacy Practices (NOP)

- The NOP describes the patient's rights and Downstate's duties in protecting those rights.
- It must be provided once to each patient at the first point of delivery of service.
- The date the NOP was given to the patient is captured in UHB's Eagle system.
- Staff members must make a good faith effort to acknowledge receipt of the NOP from the patient. The patient signs a "HIPAA Privacy Form" which is filed in the medical record.
- If the patient refuses to acknowledge receipt, the staff member should document such on this form.
- In an emergency situation, the NOP should be provided as soon as reasonably practical.
- Additional NOP's are available for HIV, mental health or alcohol & substance abuse information.
- Downstat'es NOP is posted at all points of service and is available on its website.

G. Patient Requests for Access

- Patient has a right to access all records maintained in the "designated record set", including medical records, billing records and other records used to prospectively make decisions about individual patients and their treatment.

- Patient requests for access should be directed to the Health Information Management (HIM) Department.
- Requests for inspection of records: An appointment will be made with the patient and attending physician.
- Requests for copy of records: If the request is denied, a summary of the information must be provided to the patient.
- Patient must be notified of the grounds for denial of access.
- Patient has the right to appeal and have the denial reviewed by UHB's Medical Record Committee and subsequently, by a New York State Committee.

H. Patient Requests for Additional Privacy Protections

- Patients have a right to request a restriction in the use or disclosure of their PHI for treatment, payment and healthcare operation purposes.
- Downstate is not required to agree to such restriction; however, if the request is accepted, staff members must ensure that they abide by the patient's wishes.
- Patients also have the right to request that Downstate communicate with them confidentially via an alternate address, PO Box or telephone number. Staff members should agree to such a request.

I. Patient Requests for Amendment

- Patients have the right to amend and correct their health information.
- Requests for amendment should be referred to the HIM Department.
- The attending physician and Risk Management determine whether the request should be granted.
- If the request is denied, the patient has the right to submit a statement of disagreement. Downstate can issue a rebuttal letter. All statements and rebuttals must be appended to the disputed PHI for all future uses and disclosures.

J. Personal Representatives

- Under NYS law, the following individuals qualify as "personal representatives" and are entitled to the same rights as the patient:
  - ✓ Healthcare proxy or agent;
  - ✓ Mental guardian or committee for an incompetent individual (appointed pursuant to Article 81);
  - ✓ Parent or guardian of a minor (<18 yrs);
  - ✓ Distributee of a deceased person for whom no personal representative was appointed;
  - ✓ Attorney holding a power of attorney that explicitly allows access to patient information.

- Certain documentation must be provided to ensure personal representative has appropriate authority.

K. Privacy Rights of Minors

- Parents/ guardians are granted authority over the PHI of un-emancipated minors.
- Exceptions- The minor retains control in the following circumstances:
  - ✓ Minor can lawfully obtain a healthcare service without the parent's consent, such as for treatment of sexually transmitted diseases or for abortion;
  - ✓ Parent has agreed to maintain the confidentiality between the provider and the minor in respect to a particular healthcare service.
- In a medical emergency, treatment may be provided to the minor without parental permission; however, the appropriate consents/ authorizations must be obtained after the emergency has ended.
- The attending physician may deny a parent's control if s/he reasonably believes that the minor is a victim of abuse, neglect or domestic harm by the parent.

L. Safeguards for Incidental Disclosures

- Staff members are required to put safeguards in place to protect patients' information.
- Oral patient information:
  - ✓ No professional conversations in public areas (ex: cafeteria, elevators);
  - ✓ Draw curtain and talk in low tones in semi- private rooms;
  - ✓ Intercom announcements should not link patient to a specific service or condition;
  - ✓ Never leave test results on answering machines;
  - ✓ Do not play messages via speakerphone.
- Electronic patient information:
  - ✓ Computer monitors should face away from the public;
  - ✓ Exit patient databases before leaving a workstation;
  - ✓ Never share passwords and ID's;
  - ✓ Internal emails containing PHI should be encrypted.
- Paper patient information:
  - ✓ Sign-in sheets should only contain the Name, Date & Time;
  - ✓ When placing patient charts in bins outside of patient rooms, the name should face the wall;

- ✓ Never leave PHI unattended and accessible to others, such as on conference tables or at nursing stations;
- ✓ Interoffice mail containing PHI should be sealed or stamped with a "Confidential" notice;
- ✓ All documents containing any patient information must be shredded.

M. <u>Staff Confidentiality</u>

- Staff members are required to follow all HIPAA privacy policies and procedures and complete Downstate's HIPAA training program.
- Staff members should sign, on an annual basis, the "Staff Confidentiality of Protected Health Information Statement" which is retained in the department's personnel file.
- ***A known or suspected violation of HIPAA should be reported to the appropriate supervisor, the Office of Compliance & Audit Services at x2095 or to the Confidential Compliance Hotline at 877-349-SUNY.***
- Violators will be subject to a full range of disciplinary penalties, up to and including suspension or termination.
- No retaliation will be made against an employee who reports a violation.

N. Telephone Requests for Patient Information

- If mechanisms to establish the identity and authority of a caller requesting information are unavailable, the following guidelines should be followed:
  - ✓ ***Internal requests:*** Direct the caller to the nearest workstation;
  - ✓ ***External requests:*** Request should be faxed on official letterhead to verify requestor's identity;
  - ✓ ***Patient requests:*** Request should be faxed and must contain the patient's signature.
- Sensitive information should never be disclosed via the telephone.

O. Uses & Disclosures for Treatment, Payment & Healthcare Operations (TPO)

- Uses and disclosures made for treatment of the patient, to ensure payment of healthcare services provided and to run the daily healthcare operations at Downstate are permitted without a patient's HIPAA consent.
- Treatment includes coordination of healthcare, consultation between providers and referrals. This applies to internal providers and to providers that are external to Downstate.

- Payment includes activities to obtain reimbursement for healthcare, such as billing, pre-certification and utilization review.
- Healthcare operations include operational and administrative activities, such as quality assurance, credentialing, legal review and business management.
- ***Most of the daily staff duties fall under the TPO category and do not require specific patient HIPAA consent/ authorization.***

P. <u>Uses & Disclosures Not Requiring Patient Authorization</u>

- There are certain situations where limited PHI may be disclosed to external parties without getting a patient's authorization. Examples include:
  - ✓ Disclosures required by law, such as NYS required reporting of vital events, certain lab results or types of wounds;
  - ✓ Public health activities, such as to the CDC for disease control or to notify contacts of a communicable disease;
  - ✓ Health oversight agencies, such as the DOH, for audits or inspections;
  - ✓ Victims of abuse, neglect or domestic harm to social/ protective service agencies;

- ✓ Law enforcement purposes, such as for location of a suspect or for victims of a crime.

- Refer to policy on Downstate HIPAA website for a full listing of permitted disclosures.

Q. Uses & Disclosures Requiring Patient Authorization

- A patient authorization is required for uses and disclosures that are not for treatment, payment or healthcare operations (TPO).
- Examples include sending medical records to specified individuals or selling a patient list for marketing purposes.
- Specific elements must be included on the authorization form. Therefore, Downstate's HIPAA Authorization Form, available at www.downstate.edu/hipaa must be utilized.

R. Uses & Disclosures to Individuals Involved in Care & for Notification Purposes

- Upon admission/ registration, the patient should identify an emergency contact/ next of kin regarding involvement in the patient's care.
- The contact information should be documented in the medical record and entered into UHB's Eagle system.
- If such documentation is unavailable, the following guidelines should be followed:

- ✓ ***Patient Present:*** Obtain patient's oral agreement to disclose information to an individual involved in the patient's care and document such in the patient's medical record.
- ✓ ***Patient Not Present/ Unconscious:*** Limit information disclosed to an individual involved in the patient's care to the patient's location in the facility and general condition (ie. Critical, good).

S. <u>Verification of Identity</u>

- Staff members are required to verify unknown requestors of patient information.
- Appropriate verification methods include:
  - ✓ ***Employees-*** Downstate ID;
  - ✓ ***Patients-*** Photo ID;
  - ✓ ***Public Officials-*** ID badge, agency letterhead. Department of Regulatory Affairs should be contacted.

II. Administrative Policies

A. Business Associate Agreements (BAA)

- A Business Associate (BA) is a person to whom Downstate discloses PHI so that the person can perform a function or activity on Downstate's behalf.
- Examples include contractors, consultants and system vendors.
- Business Associates must sign a Business Associate Agreement (BAA) before any PHI can be shared.
- A SUNY- approved BAA should be utilized and appended to all contracts. It is available at www.downstate.edu/hipaa.

B. Compliance & Enforcement

- In order to comply with HIPAA, Downstate will retain all necessary records and documentation.
- Downstate will cooperate with the Secretary of the Department of Health and Human Services in the event of a compliance review or investigation.

C. Covered Entity Designation

- Downstate has healthcare components and non-healthcare components.
- PHI may not be shared between the two components without specific patient authorization.
- The following entities are designated as a healthcare component and may, for

treatment, payment and healthcare operation purposes, receive patient information without specific patient authorization:

- ✓ Hospital Finance;
- ✓ Information Services
- ✓ Legal Counsel;
- ✓ Office of Compliance & Audit Services;
- ✓ Office of Institutional Advancement;
- ✓ Office of Labor Relations;
- ✓ Presidential Area;
- ✓ Student/ Employee Health Service;
- ✓ University Hospital of Brooklyn (including satellite centers);
- ✓ VP Administration;
- ✓ VP Clinical Affairs.

- Refer to complete policy located on Downstate's HIPAA website for a listing of entities designated as "non-healthcare component" where PHI disclosures require specific patient authorization.

D. Designated Record Sets

- All records used to make prospective decisions about individual patients and their treatment should be included in the "designated record set" and be made accessible to patients, when requested.
- This includes medical records, billing records and research records.

- This excludes records related to a prior examination by another provider, personal notes maintained by the provider and information disclosed to the provider by another individual in confidence on the condition that it would never be disclosed.

E. Fundraising Activities

- Fundraising includes all activities undertaken to raise money or other things of value on behalf of Downstate that requires the disclosure of PHI.
- Examples include requests for general or specific donations (such as cancer research), requests for sponsorship of events or activities, auctions and bake sales.
- The Office of Development must approve all fundraising activities.
- Physicians cannot fundraise for their own individual purpose.
- Most fundraising activities require patient authorization. However, the following information may be disclosed for this purpose without patient authorization:
  - ✓ Patient Name;
  - ✓ Address/ contact information;
  - ✓ Age and gender;
  - ✓ Insurance status;
  - ✓ Dates of treatment provided by Downstate.

F. HIPAA Training

- All State, University Physicians of Brooklyn (UPB) and Research Foundation (RF) employees, as well as residents, volunteers and any other member of Downstate's workforce must complete the HIPAA training program within two weeks of orientation.
- Individuals with access to patient information must complete the HCCS online training program available from Downstate's main web-page at www.downstate.edu.
- Individuals who do not have access to patient information must either attend the HIPAA Awareness video session presented at UHB orientation or complete the Awareness module of the online training program.
- Individuals who completed HIPAA training at another institution via the same HCCS online training program must submit documentation of completion to the Office of Compliance & Audit Services in order to achieve HIPAA compliance at Downstate.
- Residents who complete HIPAA training at Kings County must complete all modules of the HCCS online program (including HIPAA Awareness, HIPAA Privacy & HIPAA Security) within the two- week timeframe provided by Downstate at the Graduate Medical Education (GME) Orientation.

G. Marketing Activities

- Marketing activities include oral or written communications with a patient to encourage the purchase or use of a specific product or service.
- Marketing does not include communications made:
  - ✓ To describe a health related product or service provided by Downstate- such as disease management or prevention programs, health education activities and health fairs;
  - ✓ For treatment, case management and recommendations for alternative therapies or treatment.
- Most marketing activities require a specific authorization form, available at www.downstate.edu/hipaa.
- Exceptions- The following marketing activities do not require patient authorization:
  - ✓ Face to face communications, such as infant products given to mothers;
  - ✓ Promotional gifts of nominal value, such as pens and calendars.

III. Special Category Policies

A. Alcohol & Substance Abuse Information

- There are specific requirements related to the confidentiality of alcohol & substance abuse information maintained by specialized programs that provide alcohol & drug abuse treatment, diagnosis or referral for treatment.
- Refer to the complete policy available at www.downstate.edu/hipaa for a detailed delineation of the permitted uses and disclosures under HIPAA and under New York State laws, such as the Public Health Service Act and the NY Alcohol & Substance Abuse Confidentiality Law.
- Downstate's Notice of Privacy on Confidentiality of Alcohol & Substance Abuse Information and HIV Related Information should be provided to the patient.

B. HIV Information

- There are specific requirements related to the confidentiality of HIV related information, including whether an individual has been the subject of an HIV related test, has an HIV infection or HIV related illness or AIDS, or information which could reasonably identify an individual as having such a condition.
- Refer to the complete policy available at www.downstate.edu/hipaa for a detailed

delineation of the permitted uses and disclosures under HIPAA and under New York State laws, such as the NY Public Health Law, Article 27-F and NY Codes, Rules & Regulations.

- Downstate's Notice of Privacy on Confidentiality of HIV Related Information should be provided to the patient.

C. Mental Health Information

- There are specific requirements related to the confidentiality of clinical records or clinical information that identifies mental health patients.
- Refer to the complete policy available at www.downstate.edu/hipaa for a detailed delineation of the permitted uses and disclosures under HIPAA and under New York State laws, such as the NY Mental Hygiene Law.
- Downstate's Notice of Privacy on Confidentiality of Mental Health Information and Psychotherapy Notes should be provided to the patient.

D. Quality Assurance Records

- Minimum necessary guidelines should be followed for uses, disclosures and requests of PHI for quality assurance (QA) activities.
- This includes limiting unnecessary patient identifiers in QA reports and maintaining

only one copy of such reports for the QA Committee file.

- QA records should not ordinarily be maintained together with the patient's designated record set which includes the records used to make prospective decisions about a patient and which the patient has the right to access.

IV. Research Related Policies

A. Use of Limited Data Sets

- The use and disclosure of PHI that is not fully de-identified is permitted without a patient authorization for the purposes of research, public health and healthcare operations, as long as certain data elements have been removed.
- This "limited data set" involves the removal of all identifying elements listed in the policy, "De-Identification of Information"; however, it can include all elements of date and geographic subdivisions.
- A limited data set may only be used if the recipient signs a "Data Use Agreement" which protected the disclosed information. This agreement is available at www.downstate.edu/hipaa.

B. Uses & Disclosures of Decedent Information

- PHI of decedents may be used and disclosed, without authorization, for research purposes if the researcher presents:
  - ✓ Representation that the use or disclosure sought is solely for research on the PHI of decedents;
  - ✓ Documentation of the death of the patients;
  - ✓ Representation that the PHI is necessary for research purposes.

- The "Researcher Certification for PHI of Decedents" form, available at www.downstate.edu/hipaa, must be completed and placed in the patient's medical record before PHI may be disclosed.

C. Uses & Disclosures for Research

- Subject authorization is not required in the following situations, provided that the necessary documentation has been completed:
  - ✓ Reviews preparatory to research;
  - ✓ Research on decedent information;
  - ✓ IRB approval of waiver of authorization;
  - ✓ De-identified information;
  - ✓ Limited data set information.
- For all other uses and disclosures of PHI for research purposes, a specific "Research Authorization Form", available at www.downstate.edu/hipaa must be completed by the subject.
- Additional guidelines must be followed for research on genetic, HIV- related, alcohol & substance abuse, psychotherapy note and mental health information.
- Subjects generally have the right to access PHI maintained in the research record.
- Disclosures for research purposes must be documented, in accordance with the Accounting of Disclosures policy.

NOTES

PROTECTING

PATIENT PRIVACY

IS NOT ONLY OUR

OBLIGATION, IT IS

THE LAW!

DEVELOPED BY THE OFFICE OF
COMPLIANCE & AUDIT SERVICES