NEW YORK
DOWNTOWN
HOSPITAL

NEW YORK DOWNTOWN HOSPITAL
ADMINISTRATIVE POLICY & PROCEDURE MANUAL

5.06 CONFIDENTIALITY OF PATIENT INFORMATION (C-13)

Prepared/Reviewed By: Marie Cavanagh Director, Risk Management		Pages:	4
		Effective Date:	April 14, 2003
Approved By: Anthony Lisske Chief Compliance Officer		Revised/Reviewed Date(s):	5/04, 1/06, 2/08

5.06 Confidentiality of Patient Information (C-13)

POLICY

New York Downtown Hospital and its employees (full-time, part-time, temporary, contracted) medical, clinical, ancillary and volunteer staff, and officers and directors (together, "Hospital Staff") are committed to protecting the privacy and confidentiality of its patients in accordance with all relevant laws, rules and regulations, and the policies of the Hospital.

To that end, the Hospital treats "Protected Health Information" (no matter in what form it is found, including, without limitation, the medical record) as strictly confidential in accordance with the Hospital's policies, unless that information has been "de-identified" under Section D below. All Hospital Staff are responsible to preserve the confidentiality of all Protected Health Information, whether that information is in spoken, written or electronic form, and to only provide or confirm such information to someone who is authorized under the Hospital's policies, or the law, to receive the information. People who may receive such information include, among others, people who are authorized by the patient to do so, and Hospital Staff who are involved in the treatment of the patient, processing of the patient's bills, and healthcare operations.

Certain records are given additional protections with respect to confidentiality, including records of any patient in a psychiatric unit, a detoxification unit or any patient who is the subject of an HIV test, has HIV infection or an HIV-related illness (See A-6) or who has had genetic testing.

DEFINITION OF "PROTECTED HEALTH INFORMATION" (PHI)

The term “Protected Health Information” means any patient information (including very basic information such as the patient’s name or age), that

- relates to the past, present, or future physical or mental health condition of an individual, or the provision of health care to an individual, or
- relates to the past, present, or future payment for the provision of health care to an individual, and
- either identifies the individual or could reasonably be used to identify the individual.

Examples of “PHI” include:

- Clinical and psychosocial information gathered during the diagnostic/therapeutic process.
- Financial information related to the patient’s personal financial status, credit and insurance information.
- Demographic information.

PROCEDURE:

The procedures used by the Hospital to implement this policy include, but are not limited to, compliance with the protective procedures described below.

PRIVACY PRACTICES

All Hospital Staff are required to refrain from reviewing and/or discussing PHI relating to a patient’s admission, illness, treatment or condition except with other authorized personnel when necessary for performance of treatment, payment, health care operations or IRB-approved research.

Upon joining the Hospital Staff, all Hospital Staff members will sign a form detailing requirements and obligations respective to maintaining confidentiality of all Protected Health Information they may access.

All vendors with access to protected health information will sign a “business associate” agreement, which will remain on file in the department with which they do business.

Hospital Staff members will handle Protected Health Information in a manner that is consistent with the Hospital’s privacy practices as described in the then current version of the Hospital’s document entitled “Notice of Privacy Practices” that is provided to all of the Hospital’s patients. Hospital Staff members are expected to be familiar with the contents of the notice, and act accordingly.

Managerial Staff are expected to develop departmental policies and procedures with respect to the handling, and appropriate release of, Protected Health Information which are, at all times, consistent with this policy, other applicable Hospital policies, the Notice of Privacy Practices and the law.

The Notice of Privacy Practices is attached to, and considered to be a part of, this Confidentiality of Patient Information Policy.

Other than for continued patient care, healthcare operations or IRB-approved research, protected health information contained in the medical record may not be disclosed to individuals without written authorization of the patient or his/her personal representative, a subpoena, court order or a statutory requirement.

MEDICAL RECORD

The medical record, whether maintained in hard copy or electronically, is kept for the benefit of the patient, the physician and the Hospital, but it is the legal property of the Hospital. Therefore, the Hospital, subject to legal requirements, determines the policies regarding:

- The removal of the record from its designated storage site or Hospital premises.
- Who may have access to "PHI" contained in the record and how that access may be obtained.
- The kinds of information that may be taken from the medical record and the circumstances under which it may be taken.
- How access to the information will be monitored.

PUBLIC VIEWING/HEARING

Hospital Staff members are expected to keep "Protected Health Information" out of public viewing and hearing. "PHI" 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 or individuals who do not have a need to know the information.

Hospital Staff members are required to refrain from discussing "Protected Health Information" in public areas, such as the cafeteria, elevators, hallways, locker rooms, waiting rooms, etc.

Hospital staff should also take care in sharing "Protected Health Information" with families and friends of patients. PHI may generally only be shared with a family member, relative, or close personal friend who is involved in the patient's care or payment for that care. Even in these circumstances, information <u>cannot</u> be disclosed if the patient objects, or has objected, to the disclosure.

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

In order for patient information to be used or disclosed without reference to this policy and procedure, all of the following identifiers must have been properly removed from the information:

- Name (including, patient's name and those of his or her relatives, employers, and household members)
- The patients address, and all geographic subdivisions relating to the patient's address that are smaller than a State (including street address, city, county, precinct, zip code, and their equivalent geocodes other than for the initial three digits of a zip code if the geographic unit formed by such three digits contains more than 20,000 people);

- All dates related to an individual such as their birth date, admission date, discharge date, date of death, other than the calendar year; provided however, that all individuals over 89 years of age may only be aggregated into a single category of age 90 or older and may not be categorized by calendar year;
- Telephone numbers;
- Fax numbers;
- Electronic mail (e-mail) addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

In order to confirm that information being disclosed under this section has been properly de-identified, the approval of the Director of Risk Management/Privacy Officer is required prior to the disclosure or use of any de-identified information.

VIOLATIONS

Members of the Hospital Staff who violate this policy will be subject to disciplinary action up to and including termination of employment or contract with New York Downtown Hospital.

Anyone who knows or who has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the Hospital's Privacy Officer.

All reported matters will be investigated by the Hospital's Privacy Officer, and, where appropriate, steps will be taken to remedy the situation.

Where possible, New York Downtown Hospital will try to handle the reported matter confidentially.

Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract with New York Downtown Hospital.

OTHER HOSPITAL POLICIES

All Hospital Staff members are required to attend periodic in-service training on their obligations with respect to PHI.

Other Hospital policies which provide guidance regarding the handling of confidential information, including PHI are as follows:

Admin Policy and Procedure Number	Policy Name
5.06 (C-13)	Confidentiality of Patient Health Information
5.07 (C-14)	Minimum Necessary Standard Policy for Hospital Staff and Medical Staff
5.08 (C-15)	Patient Access to Medical Records
5.09 (C-16)	Release of Protected Health Information
5.10 (C-17)	Use of PHI in Treatment, Payment and Healthcare Operations
5.11 (C-18)	Business Associates: Disclosure of Protected Health Information
5.12 (C-19)	Disclosures to Family Members, Friends and/or Personal Representatives
5.13 (C-20)	Hospital Patient Directory
5.14 (C-21)	Accounting of Disclosures of Protected Health Information
5.15 (C-22)	Patient Request to Amend Protected Health Information
5.16 (C-23)	Facsimile Transmissions of Patient Health Information and Hospital Information
C-24	Use of Hospital Computer Systems, including E-mail ➡