NYU Langone MEDICAL CENTER

Issuing Department: Internal Audit, Compliance, and Enterprise Risk Management

Effective/Reissue Date: 9/13/2013

HIPAA Privacy Policy and Procedure Definitions

Definitions

The definitions below apply to all HIPAA Privacy Policies and Procedures and are derived from the HIPPA regulations. If a definition is not otherwise provided, terms will take on the meaning provided in the HIPAA regulation.

- **Authorization**: a patient's written permission to allow the Medical Center to use or disclose specified protected health information. Different types of activities (e.g. fundraising, research) have specific authorization requirements.
- **Breach**: the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule.
- **Business Associate**: a company or individual who performs a function or service on behalf of the Medical Center that creates, receives, maintains, or transmits protected health information in connection with that function or service.
- **Business Associate Agreement**: a contract between the Medical Center and a Business Associate that meets the requirement specified in the Privacy Rule.
- **Common Rule**: The Federal Policy for the Protection of Human Subjects. This regulation governs human subjects research.
- **Confidential HIV-Related Information**: is any information indicating that a patient has had an HIV-related test, has an HIV-related illness or AIDS, or has an HIV-related infection as well as any information that could reasonably identify the patient as a person who has had such a test, has an HIV-related illness or AIDS or has an HIV-related infection.
- **Disclosure**: the release, transfer, provision of access to, or divulging of information, in any manner, outside the entity holding the information.
- **De-Identified Information**: de-identified information is health information that is not subject to the same regulations as protected health information because there is no reasonable basis to believe the information could be used to identify an individual. Certain identifiers must be removed for information to be considered de-identified.
- **Designated Record Set**: a group of records maintained by or for the Medical Center that are medical records, billing records, a health plan's enrollment, payment, claims adjudication, and case or medical management records, or any group of records that is used, in whole or in part, by or for the Medical Center to make health care decisions about patients. The term *record* means any item, collection, or grouping of information

that includes PHI and is maintained, collected, used, or disseminated by or for the Medical Center.

- **Electronic Health Record**: an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.
- **Fundraising**: includes any activity undertaken to raise money or other things of value on behalf of the Medical Center. It also includes, but is not limited to: requests for donations; requests for special-purpose donations (e.g., to benefit cancer research or to remodel a reception area); requests for sponsorship of events or activities (e.g., charity dinner).
- **Genetic Information**: information about an individual's genetic tests, the genetic tests of their family members, information about a manifestation of a disease or disorder of an individual's family member. Genetic Information also include information regarding any request for or receipt of genetic services and any research participation that includes these services.
- **Health Care Operations**: refers to a variety of activities undertaken by the Medical Center in the regular course of business. It includes conducting quality assessment and improvement activities, conducting fraud and abuse detection, business planning and development, management activities and customer service.
- **Health Information**: means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
- **Health Plan**: a health plan, or insurer, means an individual or group plan that provides, or pays the cost of, medical care. This can include: a group health plan, an HMO, Medicare Part A or B, Medicaid, or a private health insurer.
- **HIM or Health Information Management**: the department that is responsible, among other things, for maintaining the Medical Center's records and access to such information.
- **IACERM or Internal Audit, Compliance, and Enterprise Risk Management**: the department that is responsible for overseeing Medical Center compliance with the HIPAA Privacy Policies and Procedures. IACERM is also responsible for breach investigations and notification.
- **Incident or Privacy/Security Incident**: the unauthorized access, use, disclosure, theft, loss, modification, or destruction of protected health information or personally identifiable information. Incidents do not always arise to the level of a breach.
- **Investigator**: an individual who is a Medical Center workforce member involved in conducting research.
- **IRB or Institutional Review Board**: the Institutional Review Board for the Medical Center which is responsible for overseeing compliance with laws and regulations for human subjects research.
- **Limited Data Set**: a set of data in which most of the personal identifiers have been removed. Certain identifiers must be removed for a data set to be considered a limited data set.

- **Marketing**: any oral or written communications with a patient about a product or service that encourages the patient to purchase or use that product or service. Marketing may also include the provision of patient information to another organization so that it may market its own products and services if the Medical Center receives direct or indirect remuneration for providing the organization with this patient information. Marketing does not include communications that are made to describe a health related product or service provided by the Medical Center for treatment purposes or for case management or care coordination purposes.
- **MCIT or Medical Center Information Technology**: The information technology department for the Medical Center. MCIT is responsible for overseeing Medical Center compliance with HIPAA security rule regulations and implementing security safeguards.
- **Medical Center or NYU Langone Medical Center**: includes NYU Hospitals Center and NYU School of Medicine. The Medical Center is designated as an Affiliated Covered Entity (ACE) which means we are one covered entity for HIPAA purposes. ACE designation allows the Medical Center to have one governing set of HIPAA policies and procedures, but also allows sharing of information for research purposes.
- **Payment**: the activities undertaken by the Medical Center to obtain or provide reimbursement for health care services it has provided. This includes billing, collection activities, and billing review activities.
- **Patient Directory**: the list of patients who are admitted to the Hospital, registered for an interventional procedure at an Article 28 outpatient space, or in the Emergency Department. This list is generated by the Medical Center's electronic health record system. An interventional procedure is any procedure requiring sedation or anesthesia, not including local anesthesia, including but not limited to the following procedures: endoscopy; catheterization; and interventional radiology.
- **Personal Representative**: a person who may legally act with authority on behalf of another person in making decisions about health care. In New York State, this is a health care surrogate under the Family Health Care Decision Act or a health care agent pursuant to a health care proxy.
- **PII or Personally identifiable information**: a person's first name or first initial and last name in combination with any of the following:
    - Social Security Number;
    - Driver's license number or other identification number; or
    - Account number or credit/debit card number with the access code or password.
- **Privacy Board**: The Medical Center IRB is designated as the Privacy Board. The Privacy Board is responsible for reviewing research protocols involving the waiver or alteration of authorizations.
- **Privacy Manager**: refers to the Medical Center designated HIPAA Privacy Official, who is responsible for overseeing compliance with HIPAA policies and procedures. The Privacy Manager is a member of the Office of Internal Audit, Compliance, and Enterprise Risk Management.
- **Privacy Rule**: refers to the HIPAA Privacy Rule, 45 C.F.R. Subpart E.
- **PHI or Protected health information**: any information (including demographic information) created, maintained, received, or transmitted by the Medical Center that

relates to health status, provision of health care or payment for health care and can be used to identify the individual.

- **Psychotherapy Notes**: are notes by a mental health professional that (1) document or analyze the contents of a conversation during a private counseling session, or during a group, joint, or family counseling session, *and* (2) that are maintained separately from the patients designated record set. If a mental health professional's notes are for any reason placed in the patient's designated record set, they are no longer psychotherapy notes.
- **Remuneration**: direct or indirect payment that flows from or on behalf of a third party whose product or service is being described. It does not include payment for the treatment of an individual. For marketing purposes, remuneration does not include non-financial or in-kind benefits. For sale of protected health information purposes, remuneration does include non-financial or in-kind benefits.
- **Research**: a systemic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. This includes: basic research studies, clinical trials, or studies involving human subjects.
- **Treatment:** the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.
- **Vendormate**: the Medical Center's Vendor Credentialing Program used to streamline the collection and management of key information regarding the business operations and representatives of our suppliers in accordance with hospital and regulatory policy.
- **Waiver or Alteration of Authorization**: the decision of a qualified IRB or Privacy Board, as evidenced by proper documentation, that states the IRB or Privacy Board has waived or altered the HIPAA requirement for patient authorization and permits the Medical Center to use of disclose the patient's PHI for research purposes.
- **Workforce Member**: employees, faculty, medical staff, residents, fellows, students, volunteers, trainees, vendors, contractors, consultants, agents, and other persons whose conduct, in the performance of work for the Medical Center, is under the direct control of the Medical Center, whether or not they are paid by the Medical Center.

Related Documents

All HIPAA Privacy Policies and Procedures

This version supersedes all previous Hospitals Center, School of Medicine, and/or Medical Center policies.