Northwestern Medicine®

Privacy & Confidentiality Policy

Subject:
GENERAL ADMINISTRATION Policy # NMHC ADM 01.0015
Version: 1.0

Title:
PRIVACY AND CONFIDENTIALITY: PATIENT, EMPLOYEE AND HOSPITAL INFORMATION
Revision of: NEW NMHC Effective Date: 04/16/2012

I. PURPOSE:

A. Subsidiaries and affiliated corporations of Northwestern Memorial HealthCare (collectively referred to in this policy as NMHC), are required to ensure that all patient, employee, and hospital information is kept confidential and secure at all times.
B. This policy identifies responsibilities of all persons affected by this policy and establishes minimum behavioral expectations for the protection of patient health information, human resources, payroll, fiscal, research, proprietary business and other management information (collectively referred to as Confidential Information) during its collection, Use, Disclosure, storage and destruction.

II. POLICY STATEMENT:

A. NMHC is committed to the protection of NMHC Confidential Information to the fullest extent while at the same time maximizing the efficiency of healthcare and business operations. This global privacy policy shall govern the management of Confidential Information by NMHC employees, local-entity medical staff, volunteers, vendors, students, residents and associated entities that support the clinical and business practices of NMHC.
B. The guidelines outlined in this policy establish a minimum set of standards for the management of Confidential Information and represent the obligations we have to our patients involving access, use and electronic communication of Confidential Information.
C. All persons affected by this policy as outlined in Section III below are required to fully document a patient's medical information in the appropriate medical record. NMHC is also obligated to maintain PHI in a safe and secure manner to protect its privacy and confidentiality. This information must be available to those individuals involved in providing patient care and business operations and must be restricted to those with a Need-to-Know. All other access is prohibited to the extent permitted by law without the patient's written Authorization.
D. Individuals with access to Confidential Information may only access such information to the extent it is necessary to perform their assigned job function and/or role, regardless of the format in which the information is obtained. Obtaining or viewing information other than what is required to do one's job is a violation of the NMHC Privacy and Confidentiality standard even if one keeps the information to oneself and does not disclose to another person.
E.All NMHC employees and persons affected by this policy as outlined in Section III below are responsible for protecting the security of all Confidential Information (oral or recorded in any form). This includes personal responsibilities for appropriately

managing assigned system user IDs and passwords and special care and good judgment in all verbal communications, particularly in public places such as elevators, cafeteria, etc. Confidential Information shall be protected during its collection, Use, storage and destruction within NMHC at all times and applies to information obtained through verbal, written and electronic means. Improper Access, Use, or Disclosure of Confidential Information – whether intentional, accidental or involuntary -- will result in investigation. Violation of this policy may be cause for immediate termination of access to further data and immediate termination of access to further data and immediate termination of employment or contract.

III. PERSONS AFFECTED:

All NMHC employees, members of each hospital entity's medical staff, house staff , students, agency personnel, volunteers and contract vendors and external construction personnel of NMHC who are responsible for business operations and/or have access to PHI, human resources, payroll, fiscal, research, proprietary and management information during its collection, Use, Disclosure, storage and destruction.

IV. PROCEDURAL RESPONSIBILITIES:

A. NMHC'S NOTICE OF PRIVACY PRACTICES

1. Each NMHC subsidiary and affiliated corporation that is a covered entity pursuant to HIPAA has an obligation to provide patients with a formal Notice of Privacy Practices (Privacy Notice). The Privacy Notice describes how the covered entity will Use and Disclose patient information for Treatment, Payment and Operational purposes. Each covered entity is required to provide a Privacy Notice to its patients and to make a good faith effort to obtain their signature acknowledging receipt of the Privacy Notice for the entity's records. In the event a Privacy Notice is provided to the patient and the patient refuses to provide a written acknowledgment, that fact will be appropriately documented and the patient will be asked to sign an acknowledgement upon their next visit to an the entity or facility.
2. Notice of Privacy Practices Guidelines is included in Appendix F.

B. ACCESS TO PATIENT INFORMATION

1. Granting access to all of NMHC's sensitive data resources, computing and data communications will be controlled based on individual user's Need-to-Know as defined by his or her job function and/or role within the organization. Access is controlled through user identification/ personal access codes, passwords and user authentication. General guidelines for providing access are as follows:

a. In general and where feasible, access to Confidential Information, will be limited to the Minimum Necessary required to fulfill or complete a task or request.

i. Minimum Necessary requirements apply to workforce access to PHI for payment and operations, requests to release PHI to external parties and release of PHI to law enforcement or for other mandated reporting requirements;

ii. Minimum Necessary requirements do not apply to the following circumstances: For treatment purposes and/or as requested by the individual to whom the information belongs as required by law. (There are exceptions to the requirement to provide information to the individual to whom the information belongs, as discussed in Appendix G).

b. For system access, individual user login and passwords must be assigned.

c. Global or departmental logins and passwords that are shared by more than one person are not permitted.

d. Where technically feasible, access to information contained in NMHC computer systems will be determined by role-based security guidelines that match the individual job function with available system functions.

e. If role-based security is not technically feasible, individual user login and passwords must be assigned based upon the judgment of the designated system administrator/manager.
f. Access/remote access to the NMHC clinical information systems is based on an established Need-to-Know basis. The granting of access to the clinical information system within NMHC does not necessarily also qualify the individual for remote access.
g. System access administrators must implement inactivity time-outs, where technically feasible, for terminals and workstations that access confidential or restricted information. The time-out interval should be based on business needs and the level of risk and exposure. Individuals should log-off workstations when finished, regardless of whether there is an automated inactivity time-out.
h. System access administrators must periodically review user access privileges and remove identification codes and passwords when users no longer require access. User access should be deactivated in the event of termination or role change within the organization.
i. Appropriate audits and review should be performed when necessary to ensure that unauthorized access and attempt to access Confidential Information is prevented.
2. Protecting and managing user access through user identifiers and passwords is a crucial element in securing NMHC Confidential Information. Guidelines for securing and managing access are as follows:
a. Individuals will safeguard and will not disclose their personal access code or any other access device that permits access to confidential patient information, e.g., never share personal access codes, passwords or devices with any other person; or allow anyone else to access or alter confidential patient information under their identity.
b. Users should not write down passwords or store them on hard copy.
c. Once access is granted, access to a function in a Clinical Information System or other information systems that contain PHI does not imply that is it proper to search this information without a Need to Know.
d. To report any lost or stolen access code or device contact the Help Desk at 312-926- HELP so it may be deactivated.
3. Access to paper medical records is subject to the same confidentiality rules and principles as applied to electronic medical records.

C. USE AND DISCLOSURE OF PATIENT INFORMATION
1. NMHC employees and other individuals affected by this Policy as described in Section III may Use and Disclose PHI for purposes related to Treatment, Payment, and Health care Operations as defined by their job function, Medical Staff privileges, or business relationship with NMHC.
2. Except for purposes outlined below, Use and Disclosure of PHI not related to TPO, may not occur with or between persons or entities without first obtaining specified Authorization or as required by law. To facilitate Disclosures that require patient Authorization, an ‘Authorization for Release of Information’ Form must be completed.
3. State and federal law may permit and/or require certain Uses and Disclosures of PHI for various purposes. The following Uses and Disclosures do not require patient Authorization pursuant to HIPAA. However, state law may be more restrictive than HIPAA with respect to certain types of “sensitive” PHI (e.g. HIV/AIDS, mental health, substance abuse treatment, genetic testing and counseling). NMHC employees must consult with the Privacy Executive for the NMHC entity involved for further guidance as to whether a specific disclosure of “sensitive PHI” is permissible under state law.
a. Health Oversight Activities: PHI may be Used or Disclosed for activities related to oversight of the health care system; government health benefits programs, and entities subject to government regulation. Activities such as audits, civil, and criminal investigations and proceedings, inspections and licensure and certification actions do not generally require a patient Authorization.

b. Public Health Activities: PHI may be Used or Disclosed to a public health authority authorized by law to collect a) reports of child abuse or neglect b) information for the purpose of preventing or controlling disease, injury or disability c) information related to vital events including adverse events or d) information to support public health surveillance, investigations or interventions.

c. Public Health Related to Abuse or Neglect Victims: Information about an individual believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority authorized to receive such reports if the individual agrees or if NMHC employees or other persons affected by this policy as outlined in Section III below believe that the information is necessary to prevent serious physical harm. The individual whose information has been released must be promptly informed that the report was made unless doing so would place the individual at risk of serious harm.

d. Serious Threats to Health or Safety: PHI may be used or disclosed if NMHC employees or other persons affected by this policy as outlined in Section III below believe that sharing the information is necessary to prevent or lessen a serious threat to a person or the general public. This type of information must be shared with someone reasonably able to prevent or lessen the threat.

e. Specialized Government Functions: PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter intelligence, and other activities authorized by the National Security Act. In addition, this information may be shared for purposes of providing protective services to the President, foreign heads of state, and others designated by law, and to support criminal investigations of threats against these persons.

f. Law Enforcement/ Court Order: PHI may be disclosed for law enforcement purposes such as when there is a court order or to inform law enforcement about a death if it is suspected that the death resulted from criminal conduct.

g. Personal Representatives: Parents or Personal Representatives have certain rights to access the PHI of the individual for whom they are legally responsible. Generally speaking, a person's right to control PHI is based on that person's right to control the individual's healthcare itself. Therefore, there are some exceptions to the general rule granting parents the right to access their child's PHI; for example, when a minor's parent or guardian doesn't control the minor's healthcare decisions that parent or guardian does not control the PHI associated with the delivery of care.

4. Other Guidelines for Use and Disclosure of Protected Health Information:

a. Business Associates: For Use and Disclosure purposes, all individuals, vendors or other entities that have been deemed " Business Associates" must follow NMHC policies and procedures on protecting NMHC patients' PHI. The Office of General Counsel, Materials Management, and individual departments/entities will determine whether a vendor is considered a Business Associate by virtue of its performance of certain functions/services on behalf of NMHC. (Refer to NMHC Contracting - Authorization, Administration and Market Evaluation Policy).

b. Research Purposes: PHI may be made available for research purposes only as approved by NMHC-affiliated Institutional Review Board (IRB) or with written patient Authorization. For further guidance on utilizing PHI for research purposes, please see the Northwestern University HIPAA policy, as well as NMH Policy 5.34: Approval to Conduct Research

c. Marketing Purposes: NMHC provides information to patients that are beneficial to them. In general, communications such as mailings reminding women to get annual mammograms, or newsletters containing information about health and wellness classes, support groups and health fairs are permitted without obtaining patient Authorization; as such activities are not considered marketing activity under HIPAA. In addition, NMHC personnel are not engaging in Marketing when they communicate to individuals about services and products offered by NMHC, for the treatment of the individual, for care coordination for individual patients, or recommendations for alternative treatments, therapies, healthcare providers or settings of care to individual patients. However, when NMHC personnel use and disclose PHI outside of the parameters above for Marketing purposes they must obtain written patient Authorization before doing so. (Refer to Appendix E.)

d. Fundraising Purposes: F undraising activities are performed solely by the Northwestern Memorial Foundation (NMF). NMF may, as part of its fundraising role, use a patient's name, address, other contact information, and the dates of

treatment provided to NMF when conducting fundraising. The use of PHI other than described above requires prior written patient Authorization to use his/her information for fundraising purposes. (See Appendix D.)

D. METHODS OF COMMUNICATING PATIENT INFORMATION

1. Internal Communication: Verbal communication should be limited to the Minimum Necessary information to meet the intended purpose, conducted with care, and only to those with a legitimate Need to Know. Extreme care should be taken when verbally discussing PHI in public places such as the cafeteria, elevators, lobby, etc. Special discretion should also be exercised when communicating information via voice mail or leaving messages on answering machines.

2. Verbal Communication: All verbal communication of PHI external to NMHC should only be conducted in emergent circumstances. When verbal release of PHI is necessitated, it must be done on a call back basis or with the use of an information access code, using the Minimum Necessary information to meet the intended purpose and only to those with a legitimate Need to Know.

3. Media Communication: All questions from the news media or other outside sources regarding patient information should be directed to an entity-specific spokesperson in the Public Relations Department. If an employee receives a request that appears questionable, he/she should immediately report the request to his/her supervisor or manager, who should then contact the entity-specific spokesperson in the Public Relations Department.

4. Electronic Communication: It is recognized that it may be useful to communicate PHI via email with physicians, nurses, lab technicians and other medical professionals associated with NMHC who are involved in providing care. Therefore, specific guidelines for the use of electronic means in communicating PHI to other NMHC employees, affiliates, or patients are provided below. Also, refer to Security Policy 1.009.

a. Physicians, Physician Assistants (PAs), and Advanced Practice Nurses (APNs) may, as part of the care process, email patients. However, PHI should be limited to the Minimum Necessary.

b. All e-mail containing PHI should be limited to the Minimum Necessary information to meet the intended purpose and directed only at NMHC personnel with a legitimate Need to Know.

c. E-mail related to patient treatments, therapies or tests should be printed and scanned into the medical record and is subject to the same scrutiny and recordkeeping that would otherwise be applied to notes in a patient chart.

d. PHI may be Used or Disclosed via the NMHC internal e-mail system for the purposes of Treatment, Payment or Health Care Operations (TPO) and must be directed at individuals within NMHC that are directly involved in TPO activities.

e. If external Disclosures or communications of PHI through e-mail (i.e., e-mails sent to individuals outside of the NMHC organization or network) are necessary for TPO activities, this communication should be done in a secure method (i.e. encryption). Please contact Information Services for guidance.

5. Fax Communication: Faxing PHI in order to facilitate care in a timely manner must be performed without compromising patient privacy and confidentiality. General guidelines for the use of Fax in communicating PHI are provided. (See Appendix C.)

E. DISPOSAL AND HANDLING OF CONFIDENTIAL INFORMATION

1. Handling of Confidential Information

a. All PHI should be kept secured at all times.

b. Individuals will not in any way use, divulge, copy, release, sell, loan, review, alter or destroy any PHI, including but not limited to non-IRB approved research or third party marketing activities, except as authorized within the scope of professional activities as a member of the NMHC staff for TPO purposes; as authorized by the patient or by his or her legal representative; or as required or permitted by law; and will not misuse or carelessly handle PHI.

2. Disposal of Confidential Information - Material that contains PHI or NMHC Confidential Information (any information that, if released prematurely or at all, could cause harm to NMHC) shall be disposed of in a manner that will ensure this information' s confidentiality. General guidelines on proper disposal are below:

a. All destruction/disposal of PHI media will be done in accordance with federal and state law and pursuant to NMHC's records management policy (01.0003 ADM). Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner. (Refer to NMHC Comprehensive IT Security Policy).

b. PHI must be personally shredded, placed in a designated locked shredding container, or disposed of using a method that ensures the patient information cannot be recovered or reconstructed. Appropriate methods for destroying/disposing of media are listed below.

i. Audiotapes: Methods for destroying/disposing of audiotapes include erasing, recycling (tape over) or destroying it completely.

ii. Computerized Data/Hard Disk Drives: Methods of destruction/disposal should erase data permanently and irreversibly.

iii. Computer Diskettes/CDs, DVDs: Methods for destroying/disposing of diskettes include reformatting, destroying, demagnetizing, or placing in locked shredding container.

iv. Microfilm/Microfiche: Methods for destroying/disposing of microfilm or microfiche include recycling and destroying (i.e. cutting).

v. PHI Labeled Devices, Containers, Name Plates, Equipment, Etc.: Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Removing or covering labels, shredding or cutting up name plates, or blacking out PHI would be appropriate.

vi. Paper Records: Paper records should be destroyed or disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include: personal shredding or placing in locked shredding container.

vii. Videotapes: Methods for destroying/disposing of videotapes include recycling (tape over) or destroying (smashing into pieces).

c. Individuals should contact their manager if they have any questions about the appropriate disposal of PHI media. Managers should notify NMHC's Office of General Counsel or the Office of Corporate Compliance &Integrity if they believe disposing information would expose NMHC to any potential wrongdoing or legal liability.

d. Individuals should not destroy, alter, or discard any media (i.e. documents) which may be subject to government investigations, audit, subpoenas, or search warrants. Standard destruction procedures should be immediately suspended once NMHC has been notified that it is part of a government investigation, or served a subpoena or search warrant.

e. If destruction/disposal services are contracted, the contract must provide that the vendor will follow the requirements imposed on it as NMHC's Business Associate as set forth in federal and state law. Furthermore, the vendor must complete a Certificate of Destruction form after each encounter and provide a copy to the appropriate NMHC department. For example, vendors responsible for shredding information will complete a Certificate of Destruction form and give it to Environmental Services. Vendors that destroy/dispose large quantities of information (i.e. medical records), not including shredding, should provide a Certificate of Destruction form to Records Management. Individuals who dispose of information in their work area or workstation (i.e. personal shredders) are not required to complete a Certificate of Destruction form.

f. Contracts between NMHC and its Business Associates must include a fully executed Business Associate Agreement, which specifies that, upon termination of the contract, Business Associates will return or destroy/dispose all PHI media.

F. MANAGEMENT OF PATIENT PRIVACY AND CONFIDENTIALITY

1. Confidentiality Agreement: A global Confidentiality Agreement (Appendix B) will be signed upon each NMHC employee's hire and employees will review the Privacy and Confidentiality policy annually. All other individuals who access the

Electronic Medical Record are also required to abide by the NMHC Privacy and Confidentiality Policy and sign Confidentiality Agreements at the time of initial contract and/or before any access to NMHC Confidential Information would occur (Appendix H)_.

2. Reporting Breaches of Security, Privacy, or Confidentiality: It is every employee's and business associate's responsibility to report suspected or known breaches of security, privacy or confidentiality. Prompt, accurate and thorough disclosure of these occurrences is not only an expectation of employees but is an obligation and a requirement of any employed position. Below are the two methods by which a breach of security, privacy, or confidentiality may be reported:

a. An individual may report a breach of security, privacy, or confidentiality by contacting and reporting full details to his/her immediate manager in accordance with the NMHC Corporate Compliance & Integrity Reporting Wrongdoing, Responsibilities and Protections Policy (ADM 1.0020). If the individual is uncomfortable talking to his/her manager or does not receive a satisfactory response from his/her manager, then the individual should talk to his/her manager's manager or may contact the entity-specific

NMHC Privacy Executive. If the individual is uncomfortable with any of these methods, the next step is to talk to the Office of Corporate Compliance & Integrity.

b. To anonymously report a suspected or known breach in security, privacy, or confidentially at any time, an individual may contact the Office of Corporate Compliance & Integrity

3. Sanctions for Breach of Security, Privacy or Confidentiality: When a breach of security, privacy or confidentiality is identified, disciplinary action may be required. Disciplinary actions should be applied in a supportive and corrective manner. In most cases, the application of disciplinary action should be directed towards improving employee performance and behavior, rather than punishing the employee. However, violations will be reviewed on an individual basis and discipline will be rendered accordingly, up to and including termination. Disciplinary action will be in accordance with entity-specific "Rules for Personal Conduct," or entity-specific Medical Staff bylaws.

4. Leadership from the applicable department and Human Resources should be consulted on the type of sanction(s) to be applied.

G. PATIENT RIGHTS: PROTECTED HEALTH INFORMATION

1. All patients have the right to access, review, and copy, amend or restrict access to their PHI as per the Guidelines set in Appendix G, Patient Rights: Protected Health Information (PHI) Policy.

2. If a patient believes information in his or her medical record is incomplete or incorrect, the patient may request an amendment to the information as outlined in Appendix G. Medical record information shall never be deleted.

3. Patients also have the right to an accounting of PHI disclosures made without their Authorization or which were not for NMHC's purposes of Treatment, Payment or Operations.

V. DEFINITIONS:

Refer to Appendix A

VI. POLICY UPDATE SCHEDULE:

Every five years or more often as appropriate

VII. REGULATORY REFERENCES:

45 CFR Part 160 and Part 164 (Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations)

VIII. APPENDICES:

Appendix A: Definitions
Appendix B: NMHC Confidentiality Agreement Appendix C: Faxing Protected Health Information (PHI)
Appendix D: Use and Disclosure of Protected Health Information (PHI) for Fundraising Activities Appendix E. Use and Disclosure of Protected Health Information (PHI) for Marketing Purposes Appendix F: Notice of Privacy Practices
Appendix G: Patient Rights Protected Health Information Appendix H: Requested Access to Electronic Medical Record

VIII. APPROVAL:

Responsible Party: Carol Pierce
Director, Health Information Management
NM Privacy Executive
Marsha Liu
Chief Integrity Executive

Reviewers:
Office of the General Counsel
Director, Operations (NMF)
Director, Marketing Director, Medical Affairs
Manager, Research
Directors, Information Services
NM Security Executive
Privacy and Security Council

Approval Party:
Timothy R. Zoph
Senior Vice President, Information Services & Chief Information Officer NMHC
Electronic Approval: 03/21/2012
Carol Lind
Senior Vice President and General Counsel
NMHC
Electronic Approval: 03/21/2012

IX. REVIEW HISTORY:

Revised: January 1, 2012 Converted to NMHC policy
Revised: November 10, 2011: No content changes. Policy number updated from 1.46 PC v08/19/2009 to current Revised: January 1, 2009
Revised: April 17, 2003

APPENDIX A: PRIVACY AND CONFIDENTIALITY POLICY DEFINITIONS

A. Authorization: Process by which a patient signs a written agreement that permits NMHC to Use or disclose their Protected Health Information (PHI), as defined below, to an entity or individual outside NMHC, as such written agreement is required by law.

B. Auto-Faxing: Automatic faxing is a computerized process that allows electronic reports to be transmitted to designated fax machines.

C. Business Associates: Individuals, vendors or organizations who perform services to or "on behalf of" NMHC that involve the Use or Disclosure of Protected Health Information. Entities deemed Business Associates require specific contractual provisions in their agreements with NMHC.

D. Confidential Information: Confidential Information is information that is collected and generated during the delivery of services and NMHC operations. It includes all information related to the operations of NMHC, including but not limited to patient records, employment records, employee information, and business, financial, proprietary and security information.

E. Designated Record Set: Record set containing protected health information that is created to respond to patients' requests concerning the information used in making decisions about them. This includes the legal medical record, billing records and other records used in whole or in part by or for the covered entity to make decisions about individuals. This does not include operational business records or clinical records from other providers.

F. Disclosure, Disclose, or Disclosing: The release, transfer, provision of access to, or divulging/ sharing of information outside of NMHC.

G. Electronic Medical Record (EMR): The electronic medical record is defined as any form of patient information that is maintained electronically by an NMHC clinical information system application (CIS).

H. Health Insurance Portability and Accountability Act of 1996 (HIPAA): A federal regulation that, among other provisions, requires that patient information be kept private and secure.

I. Marketing: Marketing is defined as a communication about a product or service that encourages the recipient of the communication to purchase or use the product or service, unless the communication is made to describe a health-related product or service that is provided by NMHC; for the treatment of the individual; or for case management or care coordination for the individual; or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

J. Minimum Necessary: During the process of requesting, Using or Disclosing PHI, reasonable efforts must be made to limit the PHI Used or Disclosed to the minimum necessary information needed to accomplish the task or intended purpose.

K. Need to Know: Information needed by an individual to provide and/or support quality patient care processes that are directed at the provision of health care to an individual; the past, present, or future payment for the provision of health care to an individual; or health care operational activities, as defined by an individual's professional responsibilities to the patient and/or the facility. Health care operations include activities such as quality improvement related initiatives, coordinating or conducting medical reviews, legal services, auditing, business planning and general business and administrative activities that support the operations of NMHC.

L. Northwestern Memorial Foundation (NMF): Raises funds to support the mission and strategic goals of NMHC

M. Notice of Privacy Practices (Privacy Notice): A document that is given to patients describing how NMH uses and discloses their medical information as well as informing patients about their rights under HIPAA.

N. Personal Representative: A person who has authority by law to make health care decisions on behalf of an adult or an emancipated minor. Under certain circumstances, an emancipated minor may be authorized by law to consent on his/her

own. There also may be occasions in which a parent or guardian acting on behalf of the minor has agreed to confidentiality between NMHC and the minor.

O. Privacy Executive: The Privacy Executive is responsible for defining, recommending, implementing and monitoring the privacy program at NMHC.

P. Protected Health Information (PHI): Individually identifiable health information is any health information, including demographic information, that can be used to identify the individual and is created or received by a health care provider, and 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. Identifiers may include: name, address, birth date, admission date, discharge date, date of death, telephone numbers, fax numbers, electronic 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.

Q. Role-Based Security: The practice of basing the level and type of access to confidential information maintained in NMHC information systems upon the individual's responsibilities or function within NMHC.

R. Role-Based Security Guidelines: Standards of practice whereby individuals' access to confidential information is limited to their job responsibilities or function within NMHC. These standards will be followed when determining and approving an individual's level of access.

S. Treatment, Payment and Operations (TPO): Treatment includes the provision, coordination, or management of heath care and related services, the consultation between providers relating to a patient, or the referral of a patient to another provider for health care. Payment includes activities performed to obtain or provide reimbursement for health care, including eligibility verification, billing, collections, medical necessity determinations and utilization review. Health care operations includes activities such as quality improvement related initiatives, the coordination or administration of medical reviews, legal services, auditing, business planning and general business and administrative activities that support the operations of NMHC.

T. Use or Using: The use or act of using information includes its collection, analysis, data transmittal, communication (verbal, written or electronic means), storage and destruction.

APPENDIX B: NORTHWESTERN MEMORIAL HEALTHCARE CONFIDENTIALITY AGREEMENT

I understand that in the course of my employment or business relationship with NMHC, it subsidiaries and affiliated corporations, I share the responsibility of maintaining the confidentiality of any patient, corporate or employee information that I may have available to me. I understand that it is my responsibility to follow any NMHC policies and procedures as they relate to the assurance of patient rights and the confidentiality of patient, corporate or employee information whether verbal, written, or electronic.

CONDUCT AND CONFIDENTIALITY:

I am responsible for conducting myself in a professional manner, ensuring the confidentiality of any information through appropriate conduct and ensuring discrete and appropriate locations for discussions of issues. I understand that release of information of any kind is dictated by the NMHC Privacy and Confidentiality Policy. If I am unsure of the policy guidelines, I will contact my manager or principal contact for direction.

PATIENT MEDICAL RECORDS AND INFORMATION:

I have read and understand the Patient Rights policy and realize my responsibility in ensuring confidentiality as outlined in that policy. I further understand that specific policies and procedures have been developed that outline the proper use and distribution of patient medical records and that I am responsible for being familiar with those documents when my job necessitates access to patient medical records. I am aware that unless specifically identified as part of my job, I am not authorized to discuss any information concerning a patient's personal data or medical condition except with other appropriate medical professionals. I am also responsible for ensuring discussions regarding patient information are held in appropriate locations with appropriate individuals.

COMPUTER SYSTEMS:

I understand that in the course of my involvement or employment, I may be required to utilize computer systems in order to fulfill my job responsibilities. If this is required, I understand that the ID number and passwords issued to me will be a unique code that identifies me for the computer systems. All inquiries and entries that I make will reference my identity and I will be fully responsible for them. Accordingly, I will maintain the confidentiality of my ID number and passwords and not reveal them to others. If at any time I feel the confidentiality of my ID number or passwords has been broken, I will contact my manager or principal contact immediately and request a new ID number and passwords. I further understand that any information I access from the computer systems is strictly confidential and to be used only in the performance of my necessary duties.

Intentional, accidental, or involuntary violation of confidentiality through verbal, written or electronic communications will result in investigation. Proven violation may be cause for immediate termination of access to further data and immediate termination of employment, subject to the terms of any collective bargaining agreement, if applicable. Any violation of confidentiality may result in legal action.

I acknowledge that I have read and understand the policy concerning the confidentiality of patient, hospital and employee information.

APPENDIX C: FAXING PROTECTED HEALTH INFORMATION (PHI)

I. GUIDELINES:

A. Faxing PHI should be limited to the minimum necessary information to meet the intended purpose.
B. Fax machines should be located in a secure location.
C. Faxing PHI internal to NMHC should be directed only to NMHC personnel with a legitimate Need to Know.
D. PHI may be faxed on a limited basis outside NMHC to individuals with a legitimate Need to Know.
Examples where faxing is appropriate include but are not limited to the following: such as:
1. For an emergent patient care encounter
2. For external placement or arrangement of services
3. For the referring physician
4. For mandated reporting requirements
5. For approval of services or to facilitate payment
E. Faxing shall not be used for routine release of information, such as, but not limited to, transmissions to insurance companies, attorneys or other non-health care entities. Incoming faxes should be disseminated to intended recipients on a regular basis.

F. Preprogrammed numbers should be validated periodically and regular fax recipients should be reminded to provide notification in the event their fax number changes.
G. Fax machines should be programmed to imprint the fax number on outgoing faxes if this function is available.
H. Auto-Faxing PHI (Scheduled Transmission of Documents by Fax)
1. All Auto-Fax receivers shall be “registered” with the initiating department to validate that patient confidentiality, appropriate authority, and secure location requirements have been met.
2. Each department that utilizes an Auto-Fax process will maintain a table of valid Auto-Faxing numbers. The fax numbers should be validated periodically and Auto-Fax recipients should be reminded to immediately notify the sending department in the event their fax number changes.
3. Departments utilizing an Auto-Faxing feature will maintain the audit reports which log the date and time of the fax, and the fax number to which the information was sent.

II. PROCEDURE:

A. Sending Documents
1. Verify the availability of the authorized receiver to receive the information before beginning the transaction.
2. Each release of information by fax should be accompanied by a cover letter including:
a. date and time of fax transmission (this may be machine generated);
b. sending facility’s name and address;
c. sending facility’s telephone and facsimile number;
d. sender's name;
e. receiving facility’s name and address;
f. receiving facility’s telephone and facsimile numbers;
g. authorized receiver’s name;
h. number of pages sent (including cover letter);
i. statement indicating that confidential health information is enclosed;
j. statement indicating that if the reader of the message is not the intended recipient, he/she is prohibited from disseminating, distributing or copying the information and should notify the sender immediately.
k. If feasible, a file should be maintained with the original cover letter and confirmation page.
3. External Misdirected Fax
a. If a fax transmission fails to reach the recipient, verify the fax number with the recipient.
b. If the misdirected fax was successfully transmitted, fax a request using the incorrect fax number, explain the information that has been misdirected, and ask for destruction or return of all documents received from NMH.
c. Complete an incident report and forward to Risk Management and the Privacy Executive.

Fax To
Date
Company Number of Pages (including cover)
From Fax number
Department Phone number
Subject Sender’s phone
CC Sender’s fax
If this message is incomplete or unclear, please notify sender Urgent Please comment
For Review Please reply

This facsimile transmission is intended for the use of the individual to whom it is addressed and may contain health information that is privileged and confidential. Any unauthorized use, disclosure, distribution, dissemination, copying or retransmission of this communication by anyone other than the intended recipient is strictly prohibited. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its slated need has been fulfilled. If you have received this transmission in error, please contact us immediately and we will arrange for its return at our expense. Thank you.

APPENDIX D: USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR FUNDRAISING ACTIVITIES

I. GUIDELINES:

A. The following patient information CAN be used for fundraising without patient authorization:

1. Name
2. Address
3. Other contact information (i.e. email address, phone number)
4. Date of service

B. The following information CANNOT be used without patient authorization:

1. Patient's diagnosis
2. Nature of services
3. Treatment
4. Place within hospital where patient receives treatment that specifically identifies that treatment, such as:

a. Department of Psychiatry
b. Department of Obstetrics
c. Department of Radiation Oncology

C. Northwestern Memorial HealthCare may use or disclose to a Business Associate, or the Northwestern Memorial Foundation (NMF), the PHI listed in item A above. NMHC will obtain an Authorization from the patient to use or disclose PHI beyond the Disclosures listed in item A above.

D. NMHC personnel and affiliated fundraising associates may use public information outside NMHC databases to send fundraising requests.

E. NMHC's Notice of Privacy Practices includes a statement that the patient's PHI may be used for fundraising purposes.

F. Fundraising communications include a statement informing the recipient that he or she may opt- out of receiving future fundraising materials with a description of how to do so.

G. NMF will make reasonable efforts to ensure patients who opt-out do not receive future fundraising communications. NMF will own and manage the suppression of names from the mailing list.

H. NMHC will sign an appropriate Business Associate contract with consultants or outside entities before disclosing patient information to those entities for fundraising activities. (See Contracting Authorization, Administering and Market Evaluation Policy 1.03). This contract is not necessary should NMHC employees or NMF perform the fundraising activities.

II. VOLUNTARY DISCLOSURE BY CONTRIBUTORS:

When a current or prospective contributor voluntarily Discloses information about diagnosis and treatment to a member of NMHC's fundraising staff, that information can then be used for other fundraising purposes.

APPENDIX E: USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR MARKETING

I. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR MARKETING

A. Using and Disclosing PHI for Marketing Purposes

1. All departments must contact their entity-specific Marketing Department before engaging in any marketing activities including but not limited to paid advertising and the hiring of advertising/creative firms. Specifically, NMHC clinical and administrative departments and affiliates should seek style guidance from the NMH Marketing Department to ensure all desired marketing tactics and/or collateral materials are developed such that they meet the NMHC brand requirements. However, note they are not required to obtain final approval to embark upon and/or initiate marketing activities.

2. NMHC does not disclose, use, sell or coerce an individual to consent to the disclosure, use, or sale of PHI for third party marketing purposes.

3. NMHC does not disclose identifiable information from a patient's medical record or financial/billing record to any non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

4. Certain activities, as described in Section B below, are not marketing as defined by HIPAA and do not require NMHC to obtain prior patient written authorization for the use or disclosure of PHI.

B. Permissible Activities

1. NMHC personnel may use and disclose PHI for these excepted activities without obtaining an authorization from the patient:

a. Mail newsletters to patients that merely promote health in a general manner and do not promote a specific product or service from a particular provider;

b. Provide information on health related products and services in a face-to-face encounter with the patient;

c. Common healthcare communications, such as disease management, care coordination for the individual, wellness programs, prescription refill reminders and appointments notifications;

d. Provide the patient with information on health care providers, settings of care, or alternative treatment options;

e. Provide sample products to the patient; and

f. Provide marketing communication involving promotional gifts of nominal value (i.e. calendars, key chains, pens, etc. that promotes a NMHC product or service).

2. Examples where patient authorization is not required:

a. Using a patient list to announce the arrival of a new facility location or the acquisition of new equipment through a general mailing or publication;

b. A primary care physician referring an individual to a specialist for a follow-up test or providing free samples of a prescription drug to a patient;

c. An endocrinologist sharing a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the individual patient. This communication is not 'marketing' as it is related to patient treatment;

d. A social worker sharing medical record information with various nursing homes in the course of recommending that the patient be transferred from a hospital bed to a nursing home;

e. Providing a free package of formula and other baby products to a new mother as they leave the maternity ward.

C. Rules for Written Marketing Communications from NMHC

1. If the marketing communication is not face-to-face but in written form, NMHC will make the determination prior to sending out the marketing communication that the product or service being marketed may be beneficial to the health of the patient.

D. Business Associates and Marketing

1. NMHC may use business associates to assist with its marketing activities; however as with any disclosure to a business associate, NMHC must obtain the business associate's agreement to use the PHI only for the communication activities and not for its own use or purpose.

E. Enforcement

1. All managers are responsible for enforcing this policy.

2. Individuals who violate this policy will be subject be subject to the disciplinary process for faculty, staff, students, or volunteers.

APPENDIX F: NOTICE OF PRIVACY PRACTICES

I. NOTICE OF PRIVACY PRACTICES GUIDELINES:

A. NMHC subsidiaries and affilaited corporations that are covered entities will follow the following guidelines on the Notice of Privacy Practices:

1. Comply with the HIPAA requirement that each individual has a right to adequate notice of the uses and disclosures of PHI that may be made, the individual's rights and NMHC's responsibilities with respect to their PHI.

2. Provide the Notice to first-time patients at all NMHC healthcare delivery sites.

3. Provide the Notice no later than the date of the first service delivery, or in an emergency treatment situation, as soon as reasonably practicable after the emergency situation has ended.

4. Provide patients with hard copy versions of the Notice in English and/or Spanish.

5. Make available printable versions of the Notice via the Intranet at NMHC's web sites in English, Spanish, Polish and Russian.

6. Make a good faith effort to obtain an initial written acknowledgment of the receipt of the Notice from the patient and document the receipt.

7. Update NMHC systems to reflect that a written acknowledgment has been secured or has not been obtained and indicate the reason why not. For example, the patient refused to sign after being requested to do so.

8. Answer patient questions regarding the content in the Notice. Employees at the care delivery sites serve as the first point for patients to ask questions about the Notice. If employees are uncertain about the response or if patients wish to speak to someone further, employees should direct patients to Patient Representatives for additional assistance.

9. Post the Notice in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice

10. Make available the Notice, upon request, whenever there is a material change to the uses and disclosures, the individual 's rights, NMHC's legal duties, or other privacy practices stated in the Notice.

B. Exceptions to Providing Notice to Patients

1. Emergency Treatment: NMHC personnel are not required to provide the Notice to patients at the time they are providing emergency treatment. During emergency situations, after the emergency situation has ended and after NMHC personnel have given patients the Notice, NMHC will make a good faith effort to obtain acknowledgment.

2. Prisoners: A prisoner receiving medical attention from NMH does not have a right to receive a copy of the Notice of Privacy Practices.

C. Documenting Patient Acknowledgment of Notice

1. NMHC must document compliance with the Notice requirements by collecting and retaining the patient's written acknowledgment that he/she received the Notice.

2. Employees, who register, admit, or secure additional information from the patient will be responsible for distributing the Notice to all patients and/or documenting the receipt of the acknowledgment.

3. NMHC will maintain the status of this activity and conduct audits to ensure compliance. Changes to departmental processes will be made, as needed.

APPENDIX G: PATIENT RIGHTS: PROTECTED HEALTH INFORMATION (PHI)

I. PROCEDURE:

A. Access, Review and Photocopying of Records

1. An individual has the right to make a written request for access, review or photocopying of their PHI in a designated record set. Use the Authorization for Release of Information Form to facilitate the request. Requests should be forwarded to the Health Information Management Department or appropriate outpatient department for processing.
2. Requests shall be acted upon within 30 days if the PHI is stored on site or within 60 days if stored in an off-site facility.
3. For access to psychiatric records, HIV test results, HIV/AIDS status, genetic tests and genetic counseling records, and substance abuse treatment, additional restrictions may apply.
4. For access to records while a patient is being treated as an inpatient, contact Health Information Management.
5. NMHC may deny access without providing an opportunity for review if the requested information consists of the following:
a. Psychotherapy notes.
b. Information compiled in anticipation of or use in a civil, criminal, or administration action or proceeding.
c. PHI subject to the Clinical Laboratory Improvements Amendments (CLIA) of 1988.
d. PHI exempt from CLIA, pursuant to 42 CFR 493.3(a)(2).
6. NMHC also may deny access without providing an opportunity for review under the following situations:
a. NMH is acting under the direction of a correctional institution and an inmate's request to obtain PHI would jeopardize the individual, other inmates, or the safety of any officer, employee, or other person at the correctional institution, or personnel responsible for transporting the inmate.
b. The individual agreed to temporary denial of access when consenting to participate in research that includes treatment and the research is not yet complete.
c. The records are subject to the Privacy Act of 1974 and the denial of access meets the requirements of that law.
d. The PHI was obtained from someone other than a healthcare provider under a promise of confidentiality and access would likely reveal the source of the information.
7. NMHC may deny access for other reasons, provided that the individual is given a right to have such denials reviewed, under the following circumstances:
a. A licensed healthcare provider has determined that the access is likely to endanger the life or physical safety of the individual or another person.
b. The PHI makes reference to another person who is not a healthcare provider and a licensed healthcare professional has determined that the access requested is likely to cause substantial harm to such other person.
c. The request for access is made by the individual's personal representative and a licensed healthcare professional has determined that access is likely to cause substantial harm to the individual or other person.
8. If access is denied for reasons listed under #7, NMHC will provide the individual with a timely written denial that contains:
a. The basis for denial.
b. How the individual can exercise his/her right to review.
c. A description of how the individual may file a complaint to NMHC and or the Secretary of Health and Human Services, Office of Civil Rights.
d. If the patient has requested a review of denial, their request will be forwarded to the Patient Representative Department for review. The patient will be notified of the determination in writing within 90 days of the request submission.

9. If the patient requests photocopies of the PHI or agrees to a summary of such information, NMHC will impose a fee that includes only the cost of:

a. Copying, including the cost of supplies for and labor of copying the PHI.

b. Postage, when the patient has requested the photocopies be mailed.

10. Patients have the right to request an electronic copy of their PHI.

B. Amendment of PHI

1. Demographic items such as spelling of name, date of birth, address, etc., may be amended by qualified personnel without written amendment request.

2. All other requests for amendment by a patient or legal representative must be submitted in writing to the Health Information Management (HIM) Department by completing the hospital Request for Amendment Form.

a. The attending physician and/or relevant caregiver will be notified of other requests for correction or amendment.

b. The response to requests for amendment to PHI will be determined by the Health Information Management Department, Office of General Counsel, the attending physician and other relevant parties.

3. The patient will be notified, in writing, within 60 days of the hospital's receipt of his/her written request for amendment, of the decision whether or not to amend the record. If the Health Information Management Department is unable to act on the amendment within 60 days, the period may be extended for no more than 30 days as long as the individual is provided with a written statement of the reasons for the delay.

4. If the request for amendment is granted, then the information will be amended, the patient will be informed of the change and others who have a Need to Know will be notified of the change. In addition, the hospital will make reasonable efforts to notify relevant persons identified by the patient of the change.

5. If the request for amendment is not granted, a written statement will be sent to the patient explaining the following:

a. The reason for denial.

b. The patient's right to submit a written statement disagreeing with the denial.

c. The patient's right to ask that the original amendment request and denial be attached to any future disclosures of the information.

d. How to file a complaint to NMHC and/or the Secretary of Health and Human Services, Office of Civil Rights.

6. Requests for amendments may be denied:

a. If the amendment request is inaccurate and/or incomplete.

b. If the PHI in question is accurate and complete.

c. If the information was not generated at Northwestern Memorial Hospital.

d. If the originator of the protected health information is no longer available to act on the requested amendment.

7. Medical record information shall never be deleted

8. The completed Request for Amendment Form will be retained with the medical record.

C. Restriction of PHI

A patient or legal representative may request that NMHC restrict the uses or disclosures of PHI about themselves to carry out treatment, payment or healthcare operations. The request for restriction must be submitted in writing to the Health Information Management Department. NMHC is not required to agree to any restriction request except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

D. Accounting of PHI Disclosures

1. A patient or legal representative has the right to receive an accounting of disclosures of PHI made by NMHC up to 6 years prior to the date on which the accounting is requested except for disclosures:

a. To carry out treatment, payment and healthcare operations
b. Of PHI made to themselves or made to others with their authorization
c. For the hospital directory or to persons involved in the patient's care or other notification purposes
d. For national security or intelligence purposes
e. To correctional institutions or other law enforcement custodial officials
f. That occurred prior to the April 14, 2003 compliance date.
2. The accounting request must be submitted in writing to the Health Information Management Department
3. The accounting must include:
a. The date of the disclosure
b. The name of the entity or person to whom the PHI was disclosed and, if known, the address of such entity or person
c. A brief description of the PHI disclosed
d. A brief statement of the purpose of the disclosure.
4. The accounting will be provided within 60 days of the request. If NMHC is unable to provide the accounting within 60 days, NMHC will provide the patient with a written statement describing the delay and will have an additional 30 days to provide the accounting.
5. The first accounting in any 12-month period will be provided without charge. Every subsequent accounting within the same 12-month period is subject to a reasonable, cost based fee.

APPENDIX H: REQUESTING ACCESS TO ELECTRONIC MEDICAL RECORD (EMR)

I. GENERAL PROCEDURE
A. ELIGIBILITY: Access to electronic patient information will be granted to an individual on a Need to Know basis. Eligible Users must only access/view information that they have a legitimate Need to Know, regardless of the extent of access provided. Need to Know is information needed to provide and/or support quality patient care processes that are directed at the provision of health care to an individual or the past, present, or future payment for the provision of health care to an individual. These processes are defined by an individual's professional responsibilities to the patient and the facility as noted below:
1. NMHC Employees
2. Volunteers, Students, Nursing, Allied Health
3. Physicians (Attendings, Resident/House staff and Medical 3rd or 4th year Students)
4. Non-NMHC Personnel (For Physician Staff support, Physicians must determine eligibility for their support staff)
5. Patient Care Consultants
6. Information System Consultants
7. Regulatory Reviewers
8. Vendors
9. For individuals not listed above who do require access to meet specific job requirements such as research, a specific patient authorization, or IRB waiver must be obtained in order to establish a Need to Know and obtain access to the EMR. Read only EMR access may be obtained by research non-employees who have fulfilled the documentation and training requirements of the NMH Research Access Program. Refer to Administrative Policy: Approval to Conduct Research) for further information. For our patients and legal guardians of patients who have the right to review their own Medical Record, these individuals may access by contacting Health Information Management / Medical Records Department.
B. REQUEST PROCEDURE

The electronic medical record is defined as any form of patient information that is maintained electronically by an NMHC Clinical Information System Application (CIS). Individuals requesting Electronic Medical Record access need to have appropriate approval and documentation to ensure they have legitimate Need to Know. The form of approval and documentation vary based on the requester's role.

C. RESPONSIBILITIES

1. It is the approvers' responsibility to inform Information Services when the approved individual is terminated or moves to a role that does not have Need to Know.
2. All individuals who access the Electronic Medical Record are required to abide by the NMHC Privacy and Confidentiality Policy and signed Confidentiality Agreements.

I have read and agree to abide by the Privacy and Confidentiality Policy regarding the importance of maintaining security, privacy and confidentiality of all protected health information, information related to business operations, and other sensitive information. I understand that non-compliance with this policy may result in corrective action as determined to be appropriate. I agree to cooperate with any investigation regarding possible privacy breaches.

Printed Name: _____

Signature: _____ Date: _____