

Subject: GENERAL ADMINISTRATION	Page 1 of 11	Policy # 1.46
Title: PRIVACY AND CONFIDENTIALITY	Revision of: 04/20/01	Effective Date: 04/17/03

I. PURPOSE:

To ensure that all patient, employee and hospital information is kept confidential and secure at all times. This policy identifies responsibilities and establishes minimum behavioral expectations for the protection of patient health information, human resources, payroll, fiscal, research, proprietary and management information during its collection, Use, Disclosure, storage and destruction within Northwestern Memorial HealthCare and its subsidiaries (“NMHC”) as defined in Section III.

II. TABLE OF CONTENTS:

I. PURPOSE 1

II. TABLE OF CONTENTS 1

III. DEFINITIONS 1

IV. POLICY STATEMENT 3

V. NMHC’s NOTICE of PRIVACY PRACTICES 4

VI. ACCESS TO PATIENT INFORMATION 4

VII. USE AND DISCLOSURE OF PATIENT INFORMATION 5

VIII. COMMUNICATING PATIENT INFORMATION 7

 A. Internal Communication 7

 B. Verbal Communication 7

 C. Media Communication 7

 D. Electronic Mail Communication 7

 E. Fax Communication 8

IX. DISPOSAL OF CONFIDENTIAL INFORMATION 8

X. MANAGEMENT OF PATIENT PRIVACY AND CONFIDENTIALITY 10

 A. Confidentiality Agreement 10

 B. Reporting Breaches of Security 10

 C. Sanctions for Breach of Privacy and Confidentiality 10

XI. APPROVALS 11

 A. Responsible Party 11

 B. Reviewers 11

 C. Approval Parties 11

III. 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.

Title: PRIVACY AND CONFIDENTIALITY	Page 2 of 11	Policy #: 1.46
---	-------------------------------	---------------------------------

- B. Business Associates: Individuals, vendors or organizations who perform services “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.
- C. 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, business, financial, proprietary and security information.
- D. Disclosure, Disclose, or Disclosing: The release, transfer, provision of access to, or divulging/sharing of information outside of NMHC.
- E. 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).
- F. 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.
- G. 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.
- H. 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 includes 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.
- I. NMHC - NMHC means Northwestern Memorial HealthCare, its subsidiaries and affiliates. This includes Northwestern Memorial Hospital (NMH), Northwestern Memorial Physicians Group (NMPG), Northwestern Memorial Home Health Care (NMHHC), and Northwestern Memorial Foundation (NMF).
- J. Organized Health Care Arrangement: For the purposes of complying with the Health Insurance Portability and Accountability Act (HIPAA), NMH, NMPG, and NMHHC have been designated as an Organized Health Care Arrangement.
- K. Personal Representatives: 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. However, 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.
- L. Privacy Executive: The Privacy Executive is responsible for defining, recommending, implementing and monitoring the privacy program at NMHC.
- M. Protected Health Information (PHI): Any patient or individually identifiable health information. Individually identifiable information is any information that can be used to identify the individual including 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 num-

Title: PRIVACY AND CONFIDENTIALITY	Page 3 of 11	Policy #: 1.46
---------------------------------------	-----------------	-------------------

bers, 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.

- N. Role-Based Security: The level and type of access to confidential information maintained in NMHC information systems is determined based upon the individual's responsibilities or function within NMHC.
- O. 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.
- P. Treatment, Payment and Operations (TPO): *Treatment* includes the provision, coordination, or management of health 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.
- Q. 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.

IV. POLICY STATEMENT:

- A. NMHC is dedicated to providing the best possible care to all patients. Patient privacy is at the core of the ***Best Patient Experience***. NMHC is committed to the protection of NMHC and patient information to the fullest extent while at the same time facilitating timely and accurate communication among our caregivers. This global privacy policy shall govern the management of confidential and proprietary information by NMHC employees, the NMH 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 are intended as the ***minimum set of expectations*** for confidentiality management. They address the privacy obligations we have to our patients, access, use and electronic communication of patient and other Confidential Information and overall management of our privacy and confidentiality program.
- C. NMHC is required to fully document a patient's medical information and maintain it 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 information about patients, employees or business matters may only obtain information that is necessary to perform their assigned job function and 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 associated with NMHC are responsible for protecting the security of all PHI and other Confidential Information (oral or recorded in any form). This includes personal responsibilities for appropriately managing assigned system user ID's and passwords and special care and good judgement in all verbal communications, particularly in public places such as elevators, cafeteria, etc. This 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. Intentional, accidental or involuntary violation of patient, employee or NMHC Confidential Information through verbal, written or electronic means will result in investigation. Proven violation may be cause for immediate termination of access to further data and immediate termination of employment or contract.

V. NMHC's NOTICE of PRIVACY PRACTICES:

- A. NMHC has an obligation to provide patients with a formal Notice of Privacy Practices (Privacy Notice). The Privacy Notice describes how NMHC will Use and disclose patient information for Treatment, Payment and Operational purposes. We are required to provide our Privacy Notice to our patients and to make a good faith effort to obtain their signature acknowledging receipt of the Privacy Notice for our records. In the event a Privacy Notice is provided to the patient and the patient refuses to provide NMHC with written acknowledgment, that fact will be appropriately documented and the patient will be asked to sign an acknowledgement upon their next visit to a NMHC facility.
- B. In emergency situations, personnel should administer medical care without delay or compromise and provide the Privacy Notice as soon as reasonably practicable after the emergency situation has ended. In addition, personnel may attempt to obtain the patient's acknowledgement of receiving the Privacy Notice only if it is determined that doing so will not compromise the patient's care. In the event acknowledgement is not obtained, personnel must attempt to obtain the patient's acknowledgement as soon as it is reasonably possible after treatment.

VI. ACCESS TO PATIENT INFORMATION:

- A. 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 their job function and 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:
 - 1. In general, information access to Confidential Information, where feasible, should be limited to the *Minimum Necessary* required to fulfill or complete a task or request.
 - a. 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;
 - b. 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.
 - 2. For system access, individual user login and passwords must be assigned.
 - 3. Global or departmental logins and passwords that are shared by more than one person are not permitted under any circumstances.
 - 4. Where technically feasible, access to information contained in our computer systems will be determined by *role-based security guidelines* which match the individual job function with available system functions.
 - 5. 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.
 - 6. Access/remote access to our Clinical Information Systems are based on an established *Need to Know* basis and are guided by a policy and procedures outlined in the Electronic Patient Information Access Policy 2.75.

7. System access administrators must implement inactivity time-outs, where technically feasible, for terminals and workstations which access confidential or restricted information. The time-out interval should be based on business needs and the level of risk and exposure. Where it is not technically feasible, individuals should log-off workstations when finished.
 8. 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.
 9. Appropriate audits and review should be performed to ensure that unauthorized access and attempt to access confidential information is prevented.
- B. Protecting and managing user access through user identifiers and passwords is a crucial element in securing our information. Guidelines for securing and managing access are as follows:
1. 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.
 2. Users should not write down passwords, store them on hard copy or keep them on a personal computer for remote log-on purposes.
 3. Once access is granted, access to a function in a Clinical Information System or other information systems that contain PHI, does not imply that it is proper to search this information at will simply to satisfy curiosity.
 4. To report any lost or stolen access code or device contact the Help Desk at 312-926-HELP so it may be deactivated.
- C. Access to paper medical records is subject to the same confidentiality rules and principles. For further guidelines, see Medical Records Policy 5.24.

VII. USE AND DISCLOSURE OF PATIENT INFORMATION:

- A. NMHC employees and other individuals associated with NMHC will Use and Disclose PHI for purposes related to Treatment, Payment, and Health care Operations as defined by their job function.
- B. Use and Disclosure of PHI not related to Treatment, Payment or Operations may not occur between persons or entities outside NMHC without first obtaining an Authorization. To facilitate Disclosures that fall under this category and require patient Authorization, an 'Authorization For Release of Information' Form must be completed.
- C. State and federal law permit and/or require certain Uses and Disclosures of PHI for various purposes without patient Authorization. For example, the following Uses and Disclosures do **not** require patient Authorization:
 1. 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 require a patient Authorization.
 2. 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 vi-

tal events including adverse events or d) information to support public health surveillance, investigations or interventions.

3. 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 the NMHC believes 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.
4. Serious Threats to Health or Safety: PHI may be used or disclosed if NMHC believes 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.
5. 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.
6. Law Enforcement/ Court Order: PHI may be disclosed for law enforcement purposes such as court order or to inform law enforcement about a death if it is suspected that the death resulted from criminal conduct.
7. 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. However, there are some exceptions, 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.

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

1. Business Associates: For Use and Disclosure purposes, all individuals, vendors or other entities who have been deemed "Business Associates" must follow NMHC policies and procedures on protecting its 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 their performance of certain functions/services on behalf of NMHC. (See Contract Administration Policy #1.40)
2. 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. NMHC personnel may discuss with patients the option of enrolling in a clinical trial without an Authorization or IRB approval. However, when the patient consents to participation in the clinical study or trial, the researcher is responsible for obtaining the patient's Authorization, unless the IRB has waived that requirement. (See Use and Disclosure of PHI for Research Purposes #1.49)
3. 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 first 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, thera-

pies, 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. (See Use and Disclosure of PHI for Marketing Purposes Policy #1.44)

4. Fundraising Purposes: Fundraising activities are performed solely by the Northwestern Memorial Foundation (NMF). NMF may, as part of their fundraising role, Use a patient's name, address, other demographic 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 Use and Disclosure of PHI for Fundraising Purposes Policy #1.42)

VIII. COMMUNICATING PATIENT INFORMATION:

- A. 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.
- B. 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, using the minimum necessary information to meet the intended purpose and only to those with a legitimate Need to Know.
- C. Media Communication: All questions from the news media or other outside sources regarding patient information should be directed to a NMHC 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 NMHC spokesperson in the Public Relations Department.
- D. Electronic Mail 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 Email in communicating PHI to other NMHC employees, affiliates, or patients are provided below (for comprehensive guidelines on the use of email at NMHC, please refer to the E-mail policy 2.70).
 - a. Physicians, Physician Assistants (PA's), and Advanced Practice Nurses (APN's) may, as part of the care process, email patients. However, adequate measures to ensure the privacy and security of clinical communications should be taken.
 - b. 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 filed in the medical record and is subject to the same scrutiny and recordkeeping that would otherwise be applied to notes in a patient's chart.
 - d. Patient PHI may be Used or Disclosed via the NMHC internal E-mail system for the purposes of treatment, payment or operations and must be directed at individuals within NMHC that are directly involved in the activities of treatment, payment or operations.
 - e. All external Disclosures or communications of PHI through E-mail (i.e., e-mails sent to individuals outside of the NMHC organization or network) are against NMHC policy and are strictly prohibited. Preferred methods for communicating PHI are fax, mail, etc.

- E. 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 below (for comprehensive guidelines on the use of fax at NMHC, please refer to the Faxing Medical Information policy 5.24.2).
1. Faxing PHI should be limited to the *Minimum Necessary* information to meet the intended purpose.
 2. PHI may be faxed outside NMHC when the information is needed on a concurrent basis such as: 1) emergent patient encounter; 2) external placement or arrangement of services; 3) by the referring physician; 4) for mandated reporting requirements or 5) for approval of services or to facilitate payment.
 3. It is critically important when faxing information that the sender has notified the recipient that a fax is on its way and that they are able to immediately retrieve the fax. Assurance should also be made that the correct fax number is used in the transmission.

IX. DISPOSAL OF CONFIDENTIAL INFORMATION:

Material which contains PHI or NMHC Confidential Information (any information which, 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 written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- B. PHI must not be discarded in trash bins, unsecured recycle bins or other publicly accessible locations. Instead this information 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 outlined in the following table.

Medium	Recommendation
Audiotapes	Methods for destroying/disposing of audiotapes include recycling (tape over) or destroying it completely.
Computerized Data/Hard Disk Drives	Methods of destruction/disposal should destroy data permanently and irreversibly. Methods may include overwriting data with a series of characters or reformatting the disk (destroying everything on it).
Computer Diskettes	Methods for destroying/disposing of diskettes include reformatting, destroying, or demagnetizing.
Microfilm/Microfiche	Methods for destroying/disposing of microfilm or microfiche include recycling and destroying (i.e. cutting)
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
Paper Records	Paper records should be destroyed/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.
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 whether it is appropriate to dispose PHI media. Managers should notify NMHC's Office of General Counsel or the Office of Corporate 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, and 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 NMHC's business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in federal and state law. Furthermore, the contracted entity 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 their business associates must provide that, upon termination of the contract, business associates will return or destroy/dispose all PHI media.

X. MANAGEMENT OF PATIENT PRIVACY AND CONFIDENTIALITY:

A. Confidentiality Agreement

A global Confidentiality Agreement (see attached), will be signed upon each employee's hire and at every performance review each year thereafter. These documents will be maintained in Human Resources personnel files. All other clinical and business associates and vendors (as appropriate) will sign a Confidentiality Agreement at the time of initial contract and/or before any access to confidential and proprietary information would occur.

B. Reporting Breaches of Security

It is every employee's responsibility to report suspected or known instances of wrongdoing. 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 an instance of wrongdoing may be reported:

1. An individual may report an instance of wrongdoing by contacting and reporting full details to their immediate manager in accordance with the NMHC Corporate Integrity Reporting Wrongdoing Policy 1.68. 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 NMHC Privacy Executive at 6-3375. If the individual is uncomfortable with any of these methods, the next step is to talk to the Office of Corporate Integrity.
2. To anonymously report a breach in security and confidentially at any time, an individual may contact Corporate Integrity Action Line at 312-926-4866.

C. Sanctions for Breach of Privacy and Confidentiality

When a breach of privacy and confidentiality is identified, disciplinary action is 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 to Policy #4.65, "Rules for Personal Conduct," or the Medical Staff bylaws.

Individuals from the applicable department, Human Resources, Risk Management and the Office of General Counsel may be consulted on the type of sanction(s) to be applied.

XI. APPROVALS:

RESPONSIBLE PARTY:

Julie Bryant
Director Medical Records
Privacy Executive
Electronically Approved: April 4, 2003

John Landreth
Corporate Integrity Executive
Electronically Approved: April 5, 2003

REVIEWERS:

Chief of Staff
Senior Vice President, Medical Affairs
Senior Vice President, Human Resources
Senior Vice President, Women's Health
Senior Vice President, Finance and Treasurer
Senior Vice President, General Counsel
Vice President, Operations and Chief Nurse Executive
Vice President, Finance
Vice President, Operations (NMPG)
Vice President, Operations (NMHHC)
Vice President, Development (NMF)
Vice President, Operations and Quality
Vice President, Operations
Director, Human Resources
Director, Marketing
Director, Research

APPROVAL PARTIES:

Tim Zoph
Vice President Information Services and CIO
Northwestern Memorial Hospital
Electronically Approved: April 14, 2003

Kathleen Murray
President & CEO
Northwestern Memorial Foundation
Electronically Approved: April 15, 2003

Dean M. Harrison
President and CEO
Northwestern Memorial Hospital
Electronically Approved: April 14, 2003

Gary Mecklenburg
President and CEO
Northwestern Memorial HealthCare
Electronically Approved: April 17, 2003