

Subject: <b>DEPARTMENTAL ADMINISTRATION</b>	Page <b>1 of 11</b>	Policy # <b>2.75</b>
Title: <b>ELECTRONIC PATIENT INFORMATION ACCESS</b>	Revision of: <b>NEW</b>	Effective Date: <b>01/09/03</b>

**I. PURPOSE:**

This policy defines general behavioral guidelines to safeguard and control the dissemination of patient information and defines procedures for access and use of electronic patient information contained in our Clinical Information Systems (CIS) and, specifically, the Electronic Medical Record (EMR). This policy outlines appropriate behaviors and expectations for use of patient information contained in any CIS application at Northwestern Memorial Hospital (NMH) and provides specific *procedures* on how to access to electronic patient information contained in our Cerner PowerChart Electronic Medical Record (EMR).

**II. DEFINITIONS:**

- A. Appropriate Access: Providing an Eligible User timely access to patient specific information that is necessary to perform his or her professional responsibilities.
- B. CIS: A collection of Clinical Information System (CIS) applications that maintain patient health information at Northwestern Memorial Hospital (NMH). Currently our CIS includes the PowerChart application. The CIS Department is an entity within Information Services which develops and maintains the Electronic Medical Record (EMR).
- C. Consultants: External Consultants to NMH will be granted access to the CIS/EMR based on 'Need to Know' as determined by a Manager or Director in the NMH department that is responsible for the work performed. For Consultants providing patient care services, access will be granted and managed by the appropriate Patient Care Department. For Information Services Consultants who provide systems and technical support to our CIS, access will be granted and managed by the CIS Department in Information Services.
- D. Eligible Individual of the EMR: Access to the Clinical Information Systems is limited to individuals performing specific patient care processes that require a 'Need to Know'.
- E. EMR: Electronic Medical Record. The electronic medical record is defined as any form of patient information that is maintained electronically by our Clinical Information System Applications (CIS).
- F. Patient information: Any patient identifiable medical data that can be viewed through an application within the Clinical Information Systems. Patient identifiable medical data includes: clinical results, patient demographics, procedures, and encounter information.
- G. Position: An application system term, the position defines the type and amount of access a user has within the CIS.
- H. Need to Know: Information needed 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 operational activities would include compliance, accreditation, licensing, certification and all other administrative activities.
- I. Regulatory Reviewers: Regulatory reviewers will be granted access to the CIS based on 'Need to Know' as determined by a Manager or Director in the Medical Records Department. The Medical Records Department will grant and manage access for regulatory reviewers performing or supporting health care operational activities.

- J. Remote Access: Application used to provide access to clinical applications through external Internet connections outside of the organization. Data viewed through Remote Access is 128 bit encrypted, complying with current industry best practices and legal standards.
- K. Secure ID: Secure Identification (ID) is a physical token used for access authentication in the Remote Access application. Secure ID is changed every 60 seconds with a randomly selected 6-digit number.
- L. Security Model: The technical structure which provides ease and timely access to patient health information, through the EMR, without compromising patient's privacy or care through inappropriate use or inadequate information.
- M. Vendors: Any organization providing goods or services to NMH, not in a consultative capacity, will be granted access to the CIS based on 'Need to Know' as determined by a Manager or Director in the Medical Records Department. Access will be granted based on the specific job function defined in the signed NMH Purchase Order or Vendor Agreement.

### III. **POLICY:**

#### A. **Security of Electronic Patient Information:**

Data security is an important consideration for everyone who utilizes the Clinical Information Systems at NMH. The electronic patient information access policy, standards and procedures specifically address confidentiality, security and protection of our clinical information. This policy applies to any individual that is granted electronic access (including remote access) to our clinical information systems and EMR at Northwestern Memorial Hospital. NMH has a legal and ethical obligation to ensure the confidentiality and security of Patient Information and individuals granted access to patient information are personally responsible for ensuring that the privacy of our patients is always protected.

#### B. **Individual Responsibilities to Ensure Confidentiality and Security:**

To ensure protection of our patient's privacy, individuals granted access to electronic patient information are required to demonstrate behavior that supports patient confidentiality at all times. Many of these behaviors are outlined in the Confidentiality Policy 1.46, our NMH Confidentiality Agreement as well as the Patient Care Policy – Medical Records 5.24. Personal obligations in this area are explained below and individuals are required to read and to abide by these duties. The violation of any of these duties will subject an individual to discipline or termination from NMH. Disciplinary action may include, but is not limited to, loss of privileges to remote access of patient information, loss of privileges at NMH, and to civil fines, penalties, judgments, and/or criminal sanctions, including imprisonment.

1. The medical record is the property of the Hospital and is maintained for the benefit of the patient, the Medical Staff and the Hospital. The information contained within the record, including all forms of electronic patient information, is the property of the patient and cannot be released to individuals not otherwise authorized, without the written consent of the patient, a subpoena, court order or statute.
2. Only authorized users with a 'Need to Know' should access clinical data on an individual patient.
3. Individuals will not misuse or carelessly care for confidential patient information or in any way use, divulge, copy, release, sell, loan, review, alter or destroy any confidential patient information. This includes, but is not limited to, non-IRB approved research or third party marketing activities, except as authorized within the scope of their professional activities as a member of the NMH medical staff for patient treatment, billing or healthcare operations; as authorized by the patient or his or her legal representative; or as required or permitted by law.

Title: <b>ELECTRONIC PATIENT INFORMATION ACCESS</b>	Page <b>3 of 11</b>	Policy # <b>2.75</b>
--	------------------------	-------------------------

4. 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. To report any lost or stolen access code or device contact the Help Desk at 312-926-HELP so it may be deactivated.

Individuals accept personal responsibility for all activities undertaken using assigned access codes or devices and will be responsible for misuse or wrongful disclosure of confidential patient information and for failure to safeguard access codes or devices.

5. For individuals who are Non-NMH personnel that directly support Physicians, the Physician or the Physician's Practice assumes responsibility for ensuring their support staff fully comply with this policy and the behaviors specifically outlined in this policy.
6. NMH has the right to monitor and audit the activities undertaken through the use of personal access codes or devices and users agree to cooperate with any investigations regarding unauthorized or improper use of confidential patient information accessed using personal access codes or devices.
7. Activities by any individual or entity that are suspected of compromising the confidentiality or security of confidential patient information must be reported. Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.
8. Personal obligations to protect our confidential information under this Agreement will continue after termination of privileges to access of patient information or loss of privileges as a member of the NMH medical staff. Access privileges hereunder are subject to periodic review, revision and if appropriate renewal.
9. Individuals have no right or ownership interest in any confidential patient information referred to in this Agreement. NMH may at any time revoke personal access codes, devices, or access to confidential patient information. At all times while exercising privileges individuals will safeguard and maintain the confidentiality of all patient information.

**C. 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. Northwestern Memorial Hospital Employees
2. Volunteers, Students, Nursing, Allied Health
3. Physicians (Attendings, Resident/House staff and Medical 3<sup>rd</sup> or 4<sup>th</sup> year Students)
4. Non-NMH 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

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. Refer to the Approval to Conduct Research patient care policy 5.43 for further information. For our patients and legal guardians of patients who have the right to review their own Medical Record, these groups may access the paper Medical Record in accordance with the Patient Care Policy # 5.24.

**D. Right to Audit**

NMH believes auditing is an essential function of safeguarding the confidential patient data from inappropriate use. Through the use of system tools and technical functionality NMH has the right, without prior notice, to conduct system audits to ensure a secure environment in which patient information is stored. The CIS Department within Information Services is responsible for the technical and physical aspects of securing patient information. NMH Medical Leadership and the Medical Records Committee are responsible for the management of processes related to auditing the EMR and reporting violations to the appropriate parties as necessary.

**E. Reporting Breaches of Security**

It is every employee’s duty 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 NMH Corporate Integrity Reporting Wrongdoing Policy 1.68. Managers will then assess the report and contact Corporate Integrity and other appropriate departments for assistance as outlined in the Reporting Wrongdoing policy.
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.

**F. Sanctions for Breach of Security**

Disciplinary action will occur in accordance to Human Resources Policy #4.65 or the Medical Staff bylaws. Corporate Integrity may involve Senior Management, Office of the General Counsel and the Director of Human Resources if necessary to facilitate an investigation.

**IV. ACCESS PROCEDURE:**

**A. Granting Access (for Cerner Powerchart EMR):**

1. Sign Appropriate Access and Confidentiality Agreement. The review and signature of an agreement outlining the basic principles of this policy and key confidentiality statements will be required in order to obtain access to NMH’s clinical information systems as well as remote access. The form necessary will depend upon the individual’s function or job responsibility (See instructions in #3-7 below).

<b>Agreement</b>	<b>Applicable Party/ Responsibility</b>
NMH Confidentiality Agreement	All individuals granted CIS/EMR access
NMH Remote Access and Confidentiality	Physicians

Agreement	
Confidentiality Contract Regarding Access to Patient Information	Non-NMH Personnel who support Physicians. Note: Physicians will be required to sign this agreement on behalf of their staff.
Vendor Access and Confidentiality Agreement	Vendors, Patient Care and Information System Consultants, Regulatory Reviewers

2. Complete Training. In general, there are two avenues through which an individual (user) may receive EMR Access. All eligible users are able to utilize either of these options:
  - a) Training Course: This course would be available after signing the NMH Confidentiality Agreement. (Refer to General Administration Confidentiality policy #1.46.) This course will teach the new user how to use the Clinical Information System as well as the importance of viewing patient data on a 'Need to Know' basis only. After completing the course the user will need to pass Competency Test.
  - b) Computer Based Training: This will be available to the user after signing the NMH Confidentiality Agreement. This CBT will teach the user how to use the Clinical Information System as well as the importance of viewing patient data on a 'Need to Know' basis only. After completing the course the user will be required to pass a Competency Test.
3. Departmental User Access to CIS: Submit **Computer Access Request Form**. The department manager (Level one or above) is the data gatekeeper for his/her department and is responsible for ensuring this policy is applied to all individuals in the department using Clinical Information Systems. Therefore, it is the responsibility of Management to determine what kind of access the employees will be granted. Once an access need is identified by the department Manager, the attached Computer Access Request Form must be completed and sent to the IS Customer Response Unit (CRU) System Administrator by the Manager. This form is also located on the NMH Intranet in the Forms folder. Access to specific system functions will then be provided based on a pre-defined role-based security access model.
4. Physician Access to CIS: Physicians will obtain, from the Medical Staff Office (MSO), a standard **NMH Confidentiality Agreement** and the **Computer Access Request Form** to review and sign. Both signed forms must be completed and sent to the CRU System Administrator. The CRU will then contact the Physician with the user login name and password.
5. Medical Students and Residents Access to CIS:

Medical Students will gain access to NMH's CIS through submission of a student list generated annually by the Associate Dean. A list of all students requiring access for the year is submitted to NMH's Customer Response Unit (CRU) for ID generation and the access codes are then distributed to all students. For Residents, Medical Affairs obtains a list of Fellows and Residents requiring access to the CIS from the University Office of Graduate Medical Education. This list is submitted to NMH's Customer Response Unit (CRU) for ID generation and the final list of access codes is distributed during Resident's Orientation or PowerChart Training Class.

Title: <b>ELECTRONIC PATIENT INFORMATION ACCESS</b>	Page <b>6 of 11</b>	Policy # <b>2.75</b>
--	------------------------	-------------------------

6. Physician Remote Access: Submit **Physician Remote Access Request Form** (for SecureID). Remote Access will provide the ability for a selected group of NMH clinical personnel to access patient information contained in the CIS through external Internet connections. To gain access to the applications, a Secure ID card is required. The user-name and PIN provide the first level of security. The Secure ID attached to the PIN to create the password for logging into Remote Access is a second level of security. The Medical Staff Office will distribute the Secure ID after a signed Remote Access and Confidentiality Agreement and Physician Remote Access Request Form has been obtained. The Secure ID card can only be obtained in person.
7. Physician Staff Remote Access: Physician will obtain, from the Medical Staff Office (MSO), a packet of information including the **NMH Confidentiality Contract Regarding Access to Patient Information, NMH Confidentiality Policy** and the **SecureID Card**. The Physician will complete the NMH Confidentiality Contract along with a list of each staff person's name, social security number and position required and return the documents to the MSO.

The Medical Staff Office will then send the Powerchart ID information with the Contract to the IS CRU (email address name: 'CRU System Admin') for processing and will send the SecureID card information to IS Security Administration (email address name: 'Secure ID Admin'). The CRU will e-mail the Physician requesting access for his/her staff the individual staff passwords. Each staff member will then read and sign the NMH Confidentiality Contract and the Physician will file and maintain this information in individual personnel files.

B. Termination of User

In the event that a user either leaves NMH, or a job change occurs where it is determined that the individual no longer needs access to electronic patient information it is the employee's Manager Responsibility to assure the user will be inactivated from all clinical information systems. (Refer to Human Resources Policy 4.77). For Physicians, the Medical Staff Office will assure that access to all clinical information systems is no longer available.

C. Transferring of NMH Roles

If a user obtains a different Human Resource position within NMH, it is the responsibility of the user's manager to verify he/she has the appropriate access needed to perform the job function.

Title: <b>ELECTRONIC PATIENT INFORMATION ACCESS</b>	Page <b>7 of 11</b>	Policy # <b>2.75</b>
--	------------------------	-------------------------

**RESPONSIBLE PARTY:**

Jody Arnoult  
Project Director, Clinical Information Systems  
Electronically Approved: October 30, 2002

**REVIEWERS:**

Information Services Vice President and Directors  
Corporate Integrity Executive  
Medical Affairs  
Medical Records Director  
Office of the General Counsel

**COMMITTEES**

IT Policy Committee

**APPROVAL PARTIES:**

Tim Zoph  
Vice President, Information Services  
Electronically Approved: October 30, 3002

Dean M. Harrison  
President & CEO, Northwestern Memorial Hospital  
Electronically Approved: January 9, 2003

## **REMOTE ACCESS AND CONFIDENTIALITY AGREEMENT**

Security and confidentiality is a matter of concern for all persons who have access to Northwestern Memorial Hospital's ("NMH") information systems. Each person accessing NMH data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. Therefore, all persons who are authorized to access data and resources, both through enterprise information systems and through individual department local area networks and databases, must read and comply with NMH policies.

Patient information is valuable and sensitive and is protected by federal and state laws and by strict NMH policies. The intent of these laws and policies is to assure that patient information will remain confidential - that is, that it will be used only as necessary to accomplish the organization's mission.

In that you have requested that NMH permit you to have remote access to confidential patient information for the purpose of patient care, you agree to conduct yourself in strict conformance to applicable state and federal laws and NMH policies governing confidential patient information. Your principal obligations in this area are explained below. You are required to read and to abide by these duties. The violation of any of these duties will subject you to discipline, which might include, but is not limited to, loss of privileges to remote access of patient information, loss of privileges at NMH, and to civil fines, penalties, judgments, and/or criminal sanctions, including imprisonment.

Accordingly, as a condition of and in consideration of NMH's provision of your remote access to confidential patient information, you promise that:

1. You will use confidential information only as needed to perform your legitimate duties as a physician of patients or a clinician in direct support of a physician affiliated with NMH. This means, among other things, that:
  - A. You will only access confidential patient information for which you have a need to know; and
  - B. You will not in any way use, divulge, copy, release, sell, loan, review, alter or destroy any confidential patient information, including but not limited to third party marketing activities, except as authorized within the scope of your professional activities as a member of the NMH medical staff for patient treatment, billing or healthcare operations; as authorized by the patient or his or her legal representative; or as required or permitted by law; and
  - C. You will only use confidential patient information for research purposes in accordance with an IRB waiver or with prior written patient authorization.
  - D. You will not misuse or carelessly care for confidential patient information.
2. You will safeguard and will not disclose your access code or any other access device that allows you to access confidential patient information, e.g., never share your access code or device with any other person; or allow anyone else to access or alter confidential patient information under your identity. You accept responsibility for all activities undertaken using your access code or device. You agree to report any lost or stolen access code or device to the Help Desk at 312-926-HELP so it may be deactivated.
3. You understand and acknowledge that NMH has the right to monitor and audit the activities undertaken through the use of your access code or device and agree to cooperate with any investigations regarding unauthorized or improper use of confidential patient information accessed using your access code or device
4. You will report activities by any individual or entity that you suspect may compromise the confidentiality or security of confidential patient information. Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.
5. You understand that your obligations under this Agreement will continue after termination of your privileges to remote access of patient information or loss of privileges as a member of the NMH medical staff. You understand that your remote access privileges hereunder are subject to periodic review, revision and if appropriate renewal.

\_\_\_\_\_ **Initial**

Title: <b>ELECTRONIC PATIENT INFORMATION ACCESS</b>	Page <b>9 of 11</b>	Policy # <b>2.75</b>
--	------------------------	-------------------------

6. You understand that you have no right or ownership interest in any confidential patient information referred to in this Agreement. NMH may at any time revoke your access code, device, or access to confidential patient information. At all times during your privileges as a member of the NMH medical staff, you will safeguard and maintain the confidentiality of all patient information.
7. **You will be responsible for your misuse or wrongful disclosure of confidential patient information and for your failure to safeguard your access code or device. You understand that your failure to comply with this Agreement may also result in loss of privileges to remote access of confidential patient information, loss of privileges, legal liability and disciplinary action or corrective action with accordance to hospital and Medical Staff policies.**

\_\_\_\_\_  
**Physician Signature**                      **Date**

\_\_\_\_\_  
**Printed Name**

**NORTHWESTERN MEMORIAL HOSPITAL**  
**CONFIDENTIALITY CONTRACT REGARDING ACCESS TO PATIENT INFORMATION**

**INTRODUCTION:**

This Confidentiality Contract has been established to ensure that access by non-NMH employees to patient information is protected and is in compliance with NMH policies, state and federal laws, and accrediting agencies. This contract is to ensure that individuals requesting access to information have been authorized and need access in order to perform their duties for patient care, continuity of care and/or administrative review.

**CONTRACT PROVISIONS:**

In that I have requested that NMH permit the designated staff members listed in Exhibit A to have access to patient information for the purpose of (please check all that apply):

- Patient care/continuing care
- Benefits/utilization/quality review
- Billing
- Other (Specify) \_\_\_\_\_

1. I agree to maintain the confidentiality of patient information in accordance with the NMH Confidentiality Policy, as amended from time to time, attached hereto as Exhibit B. I agree to keep a copy of such policies available to my staff at all times.
2. I agree to review the NMH patient information policies with my staff and instruct them as follows:
  - They are to access information only as necessary to carry out the responsibilities of their employment.
  - They are to maintain the confidentiality of patient information in accordance with the NMH Confidentiality Policy.
  - Violation of patient confidentiality may be subject to corrective action up to and including termination of employment and/or suspension and loss of privileges.
3. I agree to obtain from each one of my staff members who uses or has access to patient information a signed NM Confidentiality Statement, in the same form as that of Exhibit C, stating that he or she has been informed and understands the NMH Confidentiality Policy and will comply with such policy. I will maintain that statement in the employee's file and update it annually.
4. I agree that NMH may, at its sole discretion, revoke access to patient information at any time. I understand that access may be revoked in the event of a breach of patient confidentiality by me or any of my employees. I agree to immediately suspend or terminate further access to information by any employee if so requested.
5. I agree to adopt policies and procedures that meet the NMH standard with regard to maintaining patient information in a secure manner and properly disposing of any information which is no longer needed and which has been converted to another media, e.g., paper, tape, etc.
6. I agree that NMH may audit access to and use of its patient information by me and my staff at any time or on an ongoing basis and may ask for and receive copies of the signed employee confidentiality statement described in paragraph 3, above.
7. Special condition(s) that apply to this contract, if any, are described here:
   
\_\_\_\_\_
   
\_\_\_\_\_
   
\_\_\_\_\_
   
\_\_\_\_\_
8. This contract is effective as of the date signed and shall continue in effect for \_\_\_\_\_ (\_\_\_) year(s) subject to earlier revocation as described above or replacement by a revised contract.

- 9. I understand and agree that I shall be responsible for any violations of this Agreement by a staff member listed in Exhibit A and that I may be subject to disciplinary or corrective action in accordance with Hospital or Medical Staff policies.
- 10. My signature below indicates that I have read, understand and agree to the above provisions.

**Northwestern Memorial Hospital**

\_\_\_\_\_

**Signed By:** \_\_\_\_\_

**Signed By:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**NORTHWESTERN MEMORIAL HOSPITAL  
COMPUTER ACCESS REQUEST FORM**

**FORM INSTRUCTIONS**

1. Complete the Employee Information Section.
2. Complete any other sections for which the staff member will need access. (I.e. if a Powerchart account is needed complete the Powerchart section otherwise leave this section blank.)
3. Cut and the paste the completed form into the e-mail message. *The form should not be e-mailed as an attachment or sent from the Intranet.*
4. E-mail the completed form to "CRU System Admin" ([crumail@nmh.org](mailto:crumail@nmh.org)). The form must be e-mailed by the staff member's Level One Manager. If the staff member is a Level One Manager the Key Manager must e-mail the form. If the staff member is a Key Manager, the Senior Manager must e-mail the form.
5. For help in completing the form, please call the Customer Response Unit at 6-HELP.

**EMPLOYEE INFORMATION**

1. Employee's Name (Name should match Human Resource File)
2. Employee's Social Security Number (Social Security Number should match Human Resource File)
3. Employee's Cost Center Number (Cost Center Should match Human Resource File)
4. Employee's Job Title (Job Title should match Human Resource File)
5. Employee's Campus Address (Building, Room, Suite or Office Number and Floor)
6. Employee's Campus Phone Number (If number not yet known enter Manager's Phone Number)
7. Employee's Start Date (The Date the Employee will start in the Department)

**NETWORK ACCOUNT INFORMATION**

1. Server Name (i.e. Prentice. Enter the Name of a person in your department with an account to refer to if the server is not known)
2. Directory or file access (Enter the entire path name, i.e. (Passavant/Sys2:/Common/Bloodflow, if not known enter the name of a person in your department who has this access to refer to) Drive letters are not valid. The form may be returned if the path is not included.

**E-MAIL ACCESS**

1. Please indicate the type of E-mail this staff member will be use: Web Mail (NMCONNECT) or Regular Mail (Users that have their own PC)
2. Distribution List: (E-mail Group(s) Employee should be a member of)

***APPLICATION ACCESS (USERS WHO USE MY APPLICATIONS ONLY)***

1. Microsoft Office (Enter Yes or No)
2. MAR (Enter Yes or No)
3. MSMEDS (Enter Yes or No)

***POWERCHART ACCESS***

1. Computer Based Training Score (This is a requirement)
2. Name of Powerchart Position (Refer to the position chart for your Cost Center)