North Memorial

Maple Grove Hospital

POLICY AND PROCEDURE

Health Information Confidentiality and Security (HIPAA)

Effective Date: 05/14/2015

BUSINESS CONFIDENTIAL

Document Owner:	**Reviewed By:**	**Approved By:**
Director, HIM & Privacy Officer	Corporate Privacy Committee Corporate Compliance Committee Med Staff Exec. Committee	NMH System Leadership Team (SLT)

SCOPE

This Policy and Procedure applies to:

Ambulance Services
Clinic Services
Home and Community Services
Maple Grove Hospital
North Memorial Medical Center

POLICY

North Memorial Health Care (NMHC) protects the confidentiality, privacy and security of all patient information according to state and federal law, ethical guidelines, and industry best practices. This policy applies to each NMHC staff member, employee, volunteer, student, contractor, and vendor (collectively, "Staff"), Medical Staff and Allied Health Professionals. All managers are expected to communicate this policy to their Staff. All Staff, Medical Staff and Allied Health Professionals must be familiar with, understand, and follow the procedures in this policy.

DEFINITIONS

Confidential Information includes all patient, employee, provider, and Hospital information acquired by Staff. This includes verbal, written or electronic information obtained or otherwise recorded in any form.

A **breach** is the acquisition, access, use, or disclosure of protected health information (PHI) in a manner that compromises the security or privacy of the PHI.

Minimum necessary means limiting the use or disclosure of protected health information to the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure, or request for information.

HIM is the NMHC Health Information Management Department.

PROCEDURE

NMHC Staff must consistently ask, "Do I need to access this information in order to do my job?" If patient information is not necessary to perform your job, do not access the information.

Staff, Medical Staff and Allied Health Professionals who inappropriately access, use or disclose patient information either recklessly, out of curiosity, with malicious intent, or for other unauthorized reasons will be investigated. Any discipline will be determined, on a case-by-case basis, based on the outcome of the investigation, the individual's intent, the impact of the violation on the patient and/or NMHC, and the individual's past record of discipline, in a manner consistent with this policy. For members of the Medical Staff and Allied Health Professionals, unauthorized use and/or access to confidential information may be grounds for disciplinary action and will be reported to the Vice President/Medical Director of Medical Affairs.

Investigations in response to potential patient privacy and security violations whether through audits or requests, must be conducted in consultation with Human Resources, the manager of the Staff in question, the Privacy Officer, and, as necessary, Legal Counsel. Involvement of other internal or external parties may be necessary to complete the investigation.

Disciplinary action may include written or verbal warning, unpaid suspension, and/or termination of employment. Violation may also require notification of appropriate federal, state, or other regulatory authority, and/or licensing board. Consequences may also include and can be as severe as:

1. Permanent denial of access to the system(s).
2. Termination of medical staff privileges.
3. Criminal misuse turned-over to appropriate local, state and federal agencies (including law enforcement agencies when necessary).

Refer to Human Resources policies, bylaws, or a specific contract/business associate agreement for details about corrective and/or disciplinary action.

Types of Violations or Breaches

1. Inadvertent or unintentional violation of patient privacy/security. Violations include (but are not limited to):

   - Inadvertent access to patient records
   - Leaving a logged-in computer unattended, even if patient information is not visible

2. Actions or behaviors that are contrary to privacy/security policies or procedures or training on the topics, including careless accesses. Violations include (but are not limited to):

   - Discussing patient information with others when not required for job
   - Discussing patient information in public areas
   - Leaving logged-in computer unattended in an accessible area with patient information visible

- Improperly disposing of confidential patient information (e.g, not using confidential destruction bins)

3. Intentional access, discussion or disclosure of patient information for purposes other than patient care or authorized job function. Violations include (but are not limited to):

   - Looking up birth dates, addresses of friends or relatives
   - Accessing and reviewing a record of a patient out of concern, curiosity, or other inappropriate reasons with no need to know
   - Reviewing a high profile patient's or public personality's records
   - Multiple violations of lesser offenses
   - Sharing of user name and/or password
   - Sending identifiable patient information via unsecured e-mail
   - Capturing an image of a patient using an unauthorized personal device such as a cell phone.

4. Access, review or discussion of patient information for personal gain or with malicious intent. Violations include (but are not limited to):

   - Compiling a mailing list to be sold
   - Reviewing patient records to use information for personal reasons
   - Posting confidential information in any form to internet or on social media
   - Identity theft
   - Storing confidential information on a home computer unsecured

ACCESSING INFORMATION

A. General Confidentiality Requirements.

1. <u>All Staff must sign and comply with a confidentiality agreement.</u>

2. Staff position descriptions include language covering the expectation that each employee maintains patient and appropriate organizational confidentiality.

3. Access to information is granted based upon Staff's role. Only the "minimum necessary" information may be accessed, used, or disclosed, <u>unless</u> the information is (a) being used or disclosed for treatment purposes, (b) being disclosed to the individual who is the subject of the information, (c) being used or disclosed pursuant to a signed authorization from the patient; or (d) disclosed as part of an investigation or is a disclosure required by law or compliance with HIPAA regulations.

B. Staff Access To and Confidentiality of Health Information:

1. NMHC direct patient care staff members are authorized to access patient medical record information to provide care as required by their position and assigned unit. NMHC staff and physician/provider access to patient medical record information must only be made for the purposes of treatment, payment or healthcare operations, or when otherwise expressly permitted by law.

2. Upon patient written request, access may be restricted in the electronic medical record (EMR) through the use of an “Anonymous” flag which requires any EMR user to “Break the Glass” when attempting to access the anonymous record. Break the Glass (BTG) causes a warning to appear whenever an attempt is made to access a BTG-flagged record. If a user must access the BTG-flagged record, the user must complete the prompts, including entering the "BTG REASON" for accessing the record. NMHC uses BTG to restrict access to patient records when the patient has been seen at an affiliate clinic/hospital but not at NMHC, for legal cases, or when a patient (including employees) requests the "Anonymous" feature. NMHC HIM staff review all BTG accesses.

3. Any patient information displayed or printed from an information system of NMHC should be treated as confidential medical record information. Printed material that is no longer needed should be disposed of in a manner consistent with other printed confidential information, i.e., placed in confidential destruction bins.

4. **Capturing/duplicating of any patient information or patient image via an unauthorized electronic device (such as, but not limited to, personal cameras, video cameras, or cell phones) is prohibited.**

5. To access their own personal health records and the records of their children ages 0-10, staff are encouraged to use MyChart and to follow the Health Information Access and Disclosure policy. Staff may access their own health information for personal, non-work related reasons. Staff may access the records of their minor children ages 0 -10 without documenting any additional authorization. For children ages 11 – 17, contact the site where the child received treatment to obtain information from their records. Self-access to records of children ages 11 -17 is not allowed so that we can protect the confidentiality of records if the minor has sought confidential treatment for conditions such as sexually transmitted infections / diseases (STIs, STDs), pregnancy, alcohol / drug abuse. Access is only allowed if Staff has access to the system to perform job duties. Access is for viewing purposes only. Staff may NOT modify any transactions involving their own PHI. If Staff/patient discovers documentation that must be changed, the Staff/patient must address this through the amendment process by following steps in the Amendment of Patient Medical Records policy. Staff may not access the records of their spouse, or any family members, neighbors, friends, etc.

C. Access to the network and specific applications require unique log-ins and passwords generated by the individual user. Passwords are to be used solely in conjunction with the performance of authorized job functions. All inquiries and entries performed under the user identification and password will reference the user name.

1. A password must never be given to another individual. A password may be revised as deemed necessary by the user following an Information Technology Systems procedure.

2. Passwords will be deleted from use through Information Technology upon termination of employment or as deemed necessary by Human Resources or upon resignation/suspension of medical staff member.

3. As staff transfer within NMHC, access to applications/databases is revised and adjusted to reflect the new role.

D. Security of Electronic Health Records

1. Staff who have been authorized to read, enter, and/or update data as required by their job functions are responsible to comply with security controls and to protect confidential data from unauthorized disclosure or use.

2. Staff must exit applications when leaving computer workstations unattended. If not signed off, all computer workstations have an automatic sign-off. The timing of sign-off is determined by the system administrator/IT Division in conjunction with the application, operating system and/or platform parameters.

3. Information Technology and/or the individual database users/departments are responsible to secure the hardware and software used to run specific databases.

4. Information Technology has system integrity mechanisms in place against system crashes, lost/corrupt files, computer viruses, unauthorized access and sabotage for the major systems used by NMHC.

5. Database back-ups are completed on a regular schedule. The back-up copies are stored in a separate location from the computer.

AUDITS AND REPORTING

A. All access to patient data in the EMR and other electronic applications will be logged and permanently made available for security auditing. This applies to all staff.

B. All staff with access to the EMR are subject to random and focused audits.

1. Random audits of accesses to electronic medical records are performed in an ongoing manner by the Privacy Officer and/or designated HIM staff.

2. Focused audits are conducted to:
   a) review access to the EMR of high-profile patients;
   b) respond to a privacy or security complaint or concern; and/or
   c) review specific user access activity.

C. If you suspect that patient health information confidentiality may have been compromised, notify any individual below immediately of the concern so that appropriate action can be taken.
   1. Your manager
   2. Human Resources
   3. Privacy Officer
   4. Compliance Officer
   5. Compliance helplines:
      a. (763) 581-4670 or compliance@northmemorial.com
      b. Maple Grove Hospital: (763) 581-1575 or mghcompliance@maplegrovehospital.org
   6. Any member of NMHC leadership.

D. When a medical record has been inappropriately accessed or information has been inappropriately disclosed, the Corporate Privacy Committee will conduct an evaluation to determine if the patient should be notified.

EMERGENCY MANAGEMENT / HOSPITAL INCIDENT COMMAND SYSTEM

A. During an emergency management event, or activation of a partial/full Code Orange, it may be necessary to share certain patient information with other responding agencies (such as the American Red Cross). See Emergency Operations Plan (EOP).

REFERENCES

Corporate Code of Conduct
Corporate Compliance Program Policy
Emergency Operations Plan (EOP)
Health Information Access and Disclosure Policy
Notice of Privacy Practices
Patient Rights Policy
Performance Improvement Policy
HIM Paper-Based Record Confidentiality and Security Policy

ATTACHMENTS

Health Information Confidentiality and Security (HIPAA) - Att A - Provider Confidentiality Agreement
Health Information Confidentiality and Security (HIPAA) - Att B - NMHC Volunteer Confidentiality Agreement
Health Information Confidentiality and Security (HIPAA) - Att C - NMHC Employee Confidentiality Agreement

TABLE OF REVISIONS

Date	Description of Change(s)