MAIMONIDES MEDICAL CENTER

CODE: AD-124 (Reissued)
DATE: December 15, 2023
ORIGINALLY ISSUED: July 25, 2002

SUBJECT: CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION FOR PATIENTS AND EMPLOYEES

I. POLICY:

Maimonides Medical Center is committed to maintaining the highest level of privacy and confidentiality of health information about its patients and employees at all times and under all circumstances. Protected health information is strictly confidential and should never be given, nor confirmed, to anyone who is not authorized under the Medical Center's policies or applicable law to receive this information. Employee records and confidential Human Resource materials are strictly confidential.

II. DEFINITIONS:

"Protected health information," as used in this Policy, consists of any patient (or employee) information, including very basic information such as their name or their age, that (1) 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, and (2) either identifies the individual, or could reasonably be used to identify the individual. Protected health information may be in any form, including spoken, written, or electronic form. Examples of protected health information include, but are not limited to, medial records, medical data on information systems, and applications for health or disability benefits.

For purposes of this Policy, medical staff members include physicians as well as allied health professionals. Hospital staff members include all employees, medical or other students, trainees, residents, fellows, interns, volunteers, consultants, contractors and subcontractors at the hospital. Please note that all vendors and other business associates are considered hospital staff members for purposes of this policy.

III. RESPONSIBILITIES:

It is the responsibility of every medical staff member and hospital staff member to preserve the confidentiality of all protected health information. All medical staff and hospital staff members may share protected health information only with authorized individuals who have a "need to know" (i.e. necessary for one to perform one's specific job responsibilities adequately) in the due course of business and operations, and only in a secure area. This includes, but is not limited to, compliance with the protected procedures below.

Carelessness and Public Viewing/Hearing: Medical Staff and hospital staff are expected to keep protected health information out of public viewing and hearing.
Medical staff and hospital staff must use all efforts to ensure that they are not careless with protected health information. Carelessness occurs when an individual unintentionally or carelessly accesses, reviews, or reveals protected health information to himself/herself or others without a legitimate need to know the protected health information.

For example, protected health information should not be left in conference rooms, out on desks, or on counters or other areas where the information may be accessible to the public
or to other employees or individuals who do not have a need to know the information. Medical staff and hospital staff should also refrain from discussing protected health information in public areas, such as elevators, unless doing so is necessary to provide treatment to one or more patients.
Medical staff and hospital staff should also take care in sharing protected health information with families

and friends of patients.

Such information may generally only be shared with a family member, relative, or close personal friend who is involved in the patient's care or payment for that care. Even in these circumstances, information cannot be disclosed if the patient has objected to the disclosure.

Curiosity or Concern: Medical staff and hospital staff must not access, review and/or discuss patient information for purposes other than care of the patient. Examples include, but are not limited to, employees looking up birth dates, addresses of friends/relatives/colleagues, accessing and/or reviewing a patient record out of concern/curiosity, reviewing a "famous" or public person's record. A breach of this standard is considered a "major" breach of confidentiality.

Personal Gain or Malice: Medical staff and hospital staff must not access, review, and discuss protected health information for personal gain or with malicious intent. Examples include, but are not limited to, an employee reviews a patient record to use information in a personal relationship (could be used for sexual harassment), an employee compiles a mailing list for personal use/gain or to be sold. A breach of this standard is considered a "critical" breach of confidentiality.

Mail: Tampering with incoming or outgoing hospital mail, mail which has been placed in the distribution boxes or any communication contained in an envelope marked "confidential" is prohibited. All interdepartmental mail of a confidential nature is to be placed in a secure, confidential envelope and is to be opened only by the addressee.

Employee Information: Employee records and Human Resource materials containing protected health information are strictly confidential. Employee Human Resource files containing protected health information are to remain in the Human Resources Department secured in a locked cabinet behind a locked door with restricted access. Employee files cannot be removed from the Human Resources Department without written authorization from the Senior Vice President for Human Resources or the Vice President of Human Resources. Employee Health Services records are to be kept strictly confidential. Similarly, protected health information contained in credentialing files is to be kept strictly confidential. **An employee's or medical staff member's protected health information – is to be treated with the same respect and the same confidential manner as patient's protected health information.** Use of an employee's personal medical information (e.g. accessing employee's hospital medical record) to see if the employee was really out sick, had a doctor's appointment, or had a worker's compensation injury, is prohibited. Use of personal medical information in making employment decisions is prohibited. Breaches in employee confidential matters are the same as violating patient confidentiality and are grounds for disciplinary action up to and including termination.

Databases and Workstations: Medical Staff and hospital staff are expected to ensure that they exit any confidential database upon leaving their work stations so that protected health information is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. Medical staff and hospital staff are also expected not to disclose or release to other persons any item or process which is used to verify their authority to access or correct protected health information, including, but not limited to, any passwords, personal identification numbers, tokens or access cards, or electronic signatures.

Each medical staff member and hospital staff member will be accountable for all activity occurring under his/her account, password, and/or electronic signature. These activities may be monitored and are further described in the Medical Center's MIS Department Policies.

Downloading, Copying or Removing: Medical staff and hospital staff should not download, copy or remove from the Medical Center any protected health information.. Upon termination of employment, or contract with the hospital, or upon termination of authorization to access protected health information, medical staff members and hospital staff members must return to the Medical Center any and all copies of protected health information in their possession or under their control.

E-mailing, Texting and Faxing Protected Health Information: Medical staff and hospital staff

shall not transmit protected health information over the Internet and other unsecured networks unless using a secure encryption procedure authorized by the Medical Center. It is prohibited to use cell service provider text messaging ("SMS" or "MMS") to relay patient data between caregivers unless the technology has been sanctioned by the Medical Center. Fax transmission of protected health information should be limited to urgent situations and should be conducted only by the Health Information Services Department and those others authorized pursuant to Medical Center Policy (MED-RCDS-16) so that all necessary records can be kept for providing accountings of disclosures.

Photographs: The use of camera phones, cameras are prohibited on hospital property as they could, even, if unintended, lead to patient privacy violations. (HR 28, AD 8)

Mobile Devices: Mobile Devices include but are not limited to laptops, tablets, and smartphones. In accordance with Medical Center policy MIS-PC-014, mobile devices whether sponsored (issued by Maimonides) or non-sponsored (i.e. "BYOD" Bring Your Own Device) must have a password or be pin-configured to protect against access to PHI by unauthorized users. A non-sponsored device may not be joined to a Medical Center network and may only be connected to the Microsoft Exchange environment if the device is compliant with Active Sync configuration as outlined in the policy.

IV. **CONTROLS:**

It is the obligation of all medical staff and hospital staff to comply with the confidentiality provisions of this Policy and to contact their supervisor, or the Medical Center Legal Department, or the Privacy Officer, regarding any questions relating to this policy. The Privacy Officer has general responsibility for implementation of this Policy.

Violation of this Policy may result in disciplinary action up to, and including, termination. Anyone who knows or has reason to believe that another person has violated this Policy should report the matter promptly to his/her supervisor or the hospital's Privacy Officer. All reported matters will be investigated and, where appropriate, steps will be taken to remedy the situation. Where possible, the Medical Center will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this Policy will itself be considered a violation of this Policy that may result in disciplinary action up to and including termination.

Failure to report a breach of confidentiality will result in disciplinary action. Reporting a breach of confidentiality in bad faith or for malicious reasons will result in disciplinary action.

Kenneth D. Gibbs
President & CEO

REFERENCE:	MED-RECS-16 (Provision of Medical Records Information by Fax); AD–135 (Protection of Personal Identifying Information); HIPAA-14 (Notification of Breach of Unsecured Protected Health Information); MIS PC-14 (Mobile Device and Portable Media Policy) HIPAA SEC-017 (Removal and/or Transportation of Protected Health Information outside the Medical Center
INDEX:	Confidentiality
DEPARTMENT RESPONSIBLE:	Legal Department

H:\A JOYCE\POLICIES\AD124 (Revised 2 15 19).doc