MAIMONIDES HEALTH

CODE: HIPAA-001 (REVISED)
DATE: August 19, 2026
ORIGINALLY ISSUED: May 5, 2003

SUBJECT: PRIVACY POLICY

Contents

I. POLICY 4

II. SCOPE 4

III. DEFINITIONS 4

IV. RESPONSIBILITIES AS A COVERED ENTITY 10

A. THE PRIVACY OFFICER & OFFICE OF CORPORATE COMPLIANCE 10

B. WORKFORCE MEMBER TRAINING 10

C. INCIDENT RESPONSE TEAM 11

D. COMPLAINTS 11

V. ACCESS, USE AND DISCLOSURE OF PHI AND PII 12

A. PRIVATE INFORMATION (PI) 12

B. SOCIAL SECURITY NUMBERS (SSN) 13

C. CREDIT AND DEBIT CARD INFORMATION 13

D. ACCESS, USE AND DISCLOSURES OF PHI FOR WHICH AN AUTHORIZATION IS REQUIRED 13

i. Disclosures to Personal Representatives, Family, Friends or Others 14

ii. Disclosures Involving Sensitive Information 14

iii. Disclosures for Marketing and Fundraising Activities 16

iv. Use of Patient Information for Solicitation 17

v. Media Access to PHI 17

vi. Disclosures of PHI for Deceased Persons 18

vii. Prohibition on Photography or Recording by Patients, Family Members, Visitors and Other Third Parties 18

E. ACCESS, USE, AND DISCLOSURE OF PHI FOR WHICH AUTHORIZATION IS NOT REQUIRED 19

i. Treatment, Payment and Healthcare Operations (TPO) 19

ii. Disclosures of PHI to Business Associates (BA) 19

iii. Disclosures of Limited Data Sets (LDS) 20

iv. Disclosures of De-Identified Information 21

v. Facility Directories 21

vi. Disclosures of Employee Records and Protected Information 21

vii. Other Permissible Disclosures of PHI without Authorization: 22

F. MITIGATION OF INADVERTENT DISCLOSURES OF PHI/PII 22
G. SECURING, TRANSMITTING, RETAINING & DESTROYING PHI/PII 22
i. Safeguards and Firewalls 22
ii. Electronic Health Records 23
iii. AI and Ambient Clinical Documentation Controls 23
iv. Mailing/ Faxing/Texting 24
v. Online Tracking, Website, Mobile App, and Digital Communications Controls 24
vi. Removing PHI/PII from Maimonides Health's Premises 25
vii. Disposal of PHI/PII 26
VI. PATIENTS' HIPAA RIGHTS 26
A. NOTICE OF PRIVACY PRACTICES 26
B. ACCESS TO PROTECTED HEALTH INFORMATION 27
C. REQUESTS TO AMENDMENT 27
D. ACCOUNTING OF DISCLOSURES 28
E. REQUESTS FOR ALTERNATIVE COMMUNICATION MEANS OR LOCATION 30
F. REQUESTS FOR RESTRICTION ON USES AND DISCLOSURES OF PHI 31
i. Restricting Disclosures to a Health Plan 32
G. REQUESTS FOR A COPY OF THE PATIENT'S MEDICAL RECORD 33
i. When the Requestor is the Patient 33
ii. When the Requestor is the Patient's Personal Representative or other Qualified Person 33
H. FILING A PATIENT COMPLAINT RELATED TO PHI ACCESS, USE OR DISCLOSURE 34
VII. BREACH REPORTING 34
A. BREACH NOTIFICATION REQUIREMENTS 35
B. SECURITY BREACH OF PRIVATE INFORMATION 36
VIII. SANCTIONS FOR VIOLATIONS OF MAIMONIDES HEALTH'S PRIVACY POLICIES, PROCEDURES AND APPLICABLE LAW 37
IX. NO INTIMIDATING OR RETALIATORY ACTS; NO WAIVER OF HIPAA PRIVACY 39
X. DOCUMENTATION RETENTION 39

I. POLICY

Maimonides Health is committed to protecting the privacy and security of its Patients' Protected Health Information ("PHI") and Personally Identifiable Information ("PII"), including Private Information, (collectively "PII") in compliance with federal and state laws. The unauthorized access, use, disclosure, retention, or disposal of PHI or PII by any member of Maimonides Health may result in the erosion of patient trust as well as civil fines and/or criminal penalties. As such, anyone doing work for or on behalf of Maimonides Health, including Workforce Members and Business Associates, must maintain the confidentiality of PHI and PII in accordance with applicable laws and this Policy.

II. SCOPE

This Policy applies to all employees, agents, medical staff, volunteers, students, trainees, physician office staff, contractors, trustees and other persons performing work for or at Maimonides Medical Center, Maimonides Research and Development Foundation, MMC Holding of Brooklyn, Inc., Maimonides Health Resources, Inc., and any subsidiaries or affiliated entities, such as Brooklyn Communities Collaborative, Inc, Community Care of Brooklyn IPA, Inc, M2 Medical Community Practice, P.C. and Maimonides Midwood Community Hospital ("Maimonides Health").

III. DEFINITIONS

Artificial Intelligence ("AI") / Automated Technologies: Systems, tools, software, or services that use machine learning, natural language processing, generative AI, large language models, ambient clinical documentation, predictive analytics, agents, or similar automated functionality to create, summarize, analyze, classify, transmit, retain, or support decisions involving PHI/PII.

Ambient Clinical Documentation Technology: A tool that records, transcribes, summarizes, or drafts documentation from a clinical encounter or other patient interaction. Ambient technology may be used only if reviewed and approved through Maimonides Health's privacy, information security, legal, clinical, and contracting processes, and only in accordance with patient notice/consent workflows and approved procedures.

Breach: The unauthorized acquisition, access, use or disclosure of protected health information ("PHI") or PII which compromises the security or privacy of the PHI/PII. All unauthorized acquisitions, access, uses, or disclosures of unsecured PHI or PII will require a risk assessment to determine whether a Breach has occurred.

Business Associate ("BA"): A person or entity that on behalf of Maimonides Health (i) performs or assists in performing a function or activity involving the use and disclosure of PHI; or (ii) provides legal, accounting, actuarial, consulting, data aggregation, management (e.g., practice management, software support, utilization review, quality assurance, benefit management), administrative, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI. All BAs must enter into a Maimonides Health approved BAA or addendum unless it is determined a BAA is not required.

Business Associate Agreement ("BAA"): A legally binding agreement entered into by a Covered Entity, such as Maimonides Health, and a BA that establishes permitted and required uses and disclosures of

PHI, provides obligations for the BA to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation.

Confidential HIV-Related Information: Information protected under New York Public Health Law Article 27-F that identifies or could reasonably identify an individual as having had an HIV-related test, HIV infection, HIV-related illness, AIDS, exposure to HIV, or as a contact of a person with HIV-related information.

Covered Entity: A (i) healthcare provider; (ii) a health plan or (iii) healthcare clearing house that transmits any PHI in electronic form in connection with a transaction covered by the HIPAA Regulations.

Designated Record Set ("DRS"): Pursuant to HIPAA, means the group of records that includes PHI and is maintained, collected, used or disseminated by, or for, Maimonides Health for each individual who received care from Maimonides Health and its medical staff. The Designated Record Set includes: (i) medical or pharmacy records maintained by Maimonides Health or a Business Associate of Maimonides Health; (ii) billing records maintained by Maimonides Health or a BA of Maimonides Health; (iii) any enrollment, payment, claims adjudication, and case or medical management records maintained for a health plan or insurer by Maimonides Health or a BA of Maimonides Health; and (iv) records used in whole or in part by or for the provider to make decisions about individuals.

Disclosure of PHI: Any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to (i) persons not employed by (e.g., non-Workforce Members) or not working with Maimonides Health (e.g., not a BA of Maimonides Health) or (ii) Workforce Members or BA of Maimonides Health who do not have a legitimate business need to know the PHI.

Electronic Protected Health Information ("ePHI"): Any PHI that is covered under the HIPAA security regulations and is produced, saved, transferred or received in an electronic form.

Emancipated Minor: A Minor who is the parent of a child, or has married, or has entered the Armed Services, or is sixteen (16) years of age or older and is otherwise economically independent, or the Minor's parents have defaulted on their parental support obligations to the Minor.

Fundraising Activities: Any activities undertaken by Maimonides Health, Workforce Members, vendors, subcontractors and other BAs to raise money, or other things of value, on behalf of Maimonides Health or any of its affiliated organizations only if the activities involve the use or disclosure of PHI.

Health Insurance Portability and Accountability Act of 1996 ("HIPAA"): The federal legislation that provides data privacy (the "Privacy Rule") and security (the "Security Rule") provisions for safeguarding PHI including limits and conditions on the uses and disclosures that may be made of such information without Patient authorization. HIPAA applies to Covered Entities and their Business Associates.

Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH "): The federal legislation that strengthened the privacy provisions adopted under HIPAA, specifically extended the applicability of certain of the privacy and security rules to Business Associates, requires Patient notification for breaches of unsecured PHI, changes to permissible uses and disclosures of PHI, and

increases Patient's rights regarding access, placing restrictions on, and requesting an accounting of disclosures of their PHI.

Limited Data Set ("LDS"): PHI that excludes the following 16 direct identifiers of subject of the PHI, or of relatives, employers, or household members of the subject of the PHI: (i) names; (ii) postal address other than town, city, state and zip code; (iii) telephone numbers; (iv) fax numbers; (v) email address; (vi) social security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) web universal resource locators; (xiv) internet protocol address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images. An LDS may be used or disclosed with Institutional Review Board (IRB) approval and the execution of a Data Use Agreement, without obtaining either an individual's authorization or a waiver (or an alteration) of authorization for its access, use and disclosure. Only the following identifiers may be used in an LDS: Date (e.g., date of birth, death, or services); geographic information (except for street address); and other unique identifying numbers, characteristics or codes that are not expressly excluded.

Marketing Activities: All oral or written communications with a Patient about a product or service that encourages the Patient to purchase or use that product or service. Maimonides Health's marketing activities may involve Patient information because the marketing is directed at current or former Patients. Marketing also may include distributing Patient information to another organization so that it may market its own products and services if Maimonides Health receives direct or indirect payment in exchange for the Patient information.

Minimally Necessary: This standard requires that only the minimum amount of PHI be used, disclosed, or requested to accomplish the intended purpose or for a specific reason. This standard applies to all PHI regardless of the format in which it is maintained. Exceptions include when PHI is used or disclosed for treatment purposes, when PHI is disclosed to the individual who is the subject of the PHI or to HHS' Office for Civil Rights, when PHI is disclosed to comply with a law, or when disclosures of PHI beyond the minimum necessary are required to comply with other standards of the HIPAA Privacy Rule.

Minor: Any individual under the age of eighteen (18).

New York Stop Hacks and Improve Electronic Data Security ("SHIELD") Act: New York State data protection and breach notification law imposing data security requirements on companies that collect or maintain Private Information of New York residents.

Notice of Privacy Practices ("NPP"): The HIPAA Privacy Rule mandates that Maimonides Health distribute a Notice of Privacy Practices to all its Patients. The NPP outlines how PHI about the Patient may be used and disclosed and under what circumstances specific authorization from the Patient may not be required. The NPP also describes the HIPAA defined Patient rights related to use and disclosure of the Patient's PHI.

Outreach: A communication to describe a health-related product or service provided by Maimonides Health, or to provide general or wellness information that does not promote a particular product or service. Outreach communications may encompass population-based activities to improve health or

reduce health care costs, such as reminders to women about periodic mammograms, and communications providing information about how to lower cholesterol, new developments in health care, health or wellness classes, support groups, and health fairs.

Part 2 Records: Substance use disorder patient records subject to 42 CFR Part 2, including records maintained in connection with a federally assisted substance use disorder diagnosis, treatment, referral, prevention, rehabilitation, or research program.

Patient: As used in this Policy, shall mean the Patient, the Patient's Personal Representative and other Qualified Persons as defined under New York State law.

Personal Representative: The person who, for decision-making purposes, will be treated as the Patient. Depending on the circumstances of each case, the Personal Representative may be directly appointed by the Patient or may be deemed to serve the role of Personal Representative under applicable laws and regulations.

Personally Identifiable Information ("PII"): Any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify that person. Personal information may include demographic, contact, employment, financial, online account, biometric, medical, health insurance, or other identifying information, whether maintained in paper, electronic, oral, or other form.

Private Information ("PI"): Personal Information combined with one or more protected data elements, where either the Personal Information or the protected data element is not encrypted, or is encrypted with an encryption key that has also been access or acquired. Under the New York State Shield Act and related New York requirements, protected data elements include, as applicable : (i) Social Security number; (ii) driver's license number or non-driver identification card number; (iii) Account number, credit or debit card number, with or without a security code, access code, or password where the number could be used to access an individuals' financial; (iv) biometric information (e.g., fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data used to authenticate or ascertain the individual's identity; (v) medical information; (vi) health insurance information (e.g., insurance policy number, subscriber identification number, any unique identifier used by a health insurer to identify the individual or any information in an individual's application and claims history); and (vii) a user name or mail address in combination with a password or security question and answer that would permit access to an online account. For purposes of this Policy, Private information also includes other sensitive identifiers or access-enabling information maintained by Maimonides Health (e.g., mother's maiden name or surname prior to marriage, home address, telephone numbers, email address, internet ID name, ATM numbers or codes, electronic serial numbers, personal identification numbers, and any information that would permit access to an individual's financial accounts).

Protected Health Information ("PHI"): Information that is created or received by Maimonides Health and relates to the past, present, or future physical or mental health or condition of a Patient, the provision of health care to a Patient, or the past, present, or future payment for the provision of health care to a Patient. PHI can be written or oral; it can be recorded on paper, computer or removable or

other media. HIPAA further clarifies that PHI includes information that identifies the Patient by one or more (depending on context) of the following 18 identifiers:

1. Names;
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code in certain situations;
3. All elements of date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers;
13. Medical Device Identifiers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

PHI includes such information with regard to deceased individuals, unless the individual has been deceased for longer than fifty (50) years. PHI does not include employment records held by Maimonides Health in its capacity as an employer, or information that has been de-identified in accordance with the HIPAA Privacy Standards.

Qualified Persons: As defined in New York State, means:

- A guardian for an incapacitated person (NYMHL Article 81);
- A conservator/committee appointed to represent the needs of an incompetent Patient;
- An administrator or executor of a deceased Patient, who should provide a copy of letters of Administration or Letters Testamentary along with a HIPAA authorization form;
- A parent of an infant, a guardian of an infant appointed by NY Surrogate's Court Procedure Act Article 17 or any other legally appointed guardian of an infant who may be entitled to request access to a clinical record;
- A distributee of a deceased Patient's estate who provides a copy of the Patient's death certificate and an affidavit that an estate representative has not been appointed;
- An attorney representing or acting on behalf of the Patient or the Patient's estate who holds a power of attorney from the Qualified Person or the Patient's estate explicitly authorizing the holder to execute a written request for Patient information.

Recording: A recording an individual's likeness (e.g., image or picture) or voice using photography (e.g., cameras or cellular telephones), audio recording (e.g., a tape or digital recorder), video recording (e.g., video cameras or cellular telephones), digital imaging (e.g., digital cameras or web cameras), or other technologies capable of capturing an image or audio data (e.g., Skype).

Regional Health Information Organization ("RHIO") / Qualified Entity ("QE") / SHIN-NY: A certified regional health information organization or other qualified entity participating in the Statewide Health Information Network for New York (SHIN-NY), including Healthix where applicable, that enables electronic exchange of patient information for authorized purposes under 10 NYCRR Part 300 and applicable SHIN-NY policy guidance.

Reproductive Health Information. Includes information relating to abortion services, contraception, pregnancy-related services, fertility services, sexually transmitted infection services, and other reproductive healthcare.

Sale of PHI: A disclosure of PHI by Maimonides Health, or a Business Associate of Maimonides Health, if applicable, where Maimonides Health or its Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. Remuneration includes both financial and non-financial benefits.

Sanctions: Progressive disciplinary actions, up to and including termination, taken by Maimonides Health against an individual who has been identified as violating this Policy.

Security Breach: The unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of Private Information.

Senior Management: Director and above.

Tracking Technologies: Website, patient portal, mobile application, email, advertising, analytics, cookie, pixel, session-replay, software development kit, or similar technology that collects, transmits, or permits access to information about an individual's interactions with Maimonides Health digital properties.

Treatment, Payment, or Healthcare Operations ("TPO") Purposes: Includes the following primary circumstances under which Workforce Members may access, use and disclose an individual's PHI/PII without a signed Authorization.

- **Treatment**: The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a Patient, or the referral of a Patient for health care from one health provider to another.
- **Payment**: The access, use or disclosure of PHI/PII as necessary to receive reimbursement or compensation for services provided. Includes contacting an insurer to get Payment authorization for services provided, billing individuals for the cost of services it has provided, and as necessary for another Covered Entity's Payment activities as long as both Maimonides Health and the other Covered Entity have or had a relationship with the subject of the PHI being disclosed, the PHI pertains to such relationship, and the disclosure is for (i) conducting quality assessment and improvement activities, (ii) patient safety activities, (iii) population- based activities relating to improving health or reducing health care costs, protocol development, case

management and care coordination, contacting of health care providers and individuals with information about Treatment alternatives; related functions that do not include Treatment; (v) reviewing the competence or qualification of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioner in area of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities; (vi) the purpose of health care fraud and abuse detection or compliance.

- **Healthcare Operations**: The access, use and disclosures for Maimonides Health's own operations, including, but not limited to, quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, activities related to contracting for health insurance or health benefits, conducting or arranging for medical review, legal review, or auditing functions, business planning and development, business management and administrative activities.

Use of PHI: Includes the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any Workforce Member, or by a BA of Maimonides Health.

Workforce Members: Individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of Maimonides Health, whether or not they are paid by Maimonides Health. The term "employee" or "staff" includes all of these types of workers.

IV. RESPONSIBILITIES AS A COVERED ENTITY

A. THE PRIVACY OFFICER & OFFICE OF CORPORATE COMPLIANCE

Maimonides Health's Privacy Officer is responsible for (i) monitoring Maimonides Health's compliance with privacy laws, including HIPAA, 42 CFR Part 2, NYS SHIELD Act, and NYS Hospital Cybersecurity Regulation, and this Policy; (ii) developing and implementing of policies and procedures relating to privacy of PHI/PII and Private Information; and (iii) working with other departments to investigate and resolve privacy-related complaints from Patients, their representatives, family members, Workforce Members, or other individuals.

The Privacy Officer and Office of Corporate Compliance work with several departments in Maimonides Health to protect the privacy and security of PHI, including:

- The Office of Legal Affairs ("OLA"): In conjunction with the Privacy Officer, the OLA is responsible for ensuring that Maimonides Health complies with the provisions of the HIPAA Privacy Rule regarding third-party business associate vendors or subcontractors, including the requirement that a HIPAA-compliant Business Associate Agreement is in place with BA vendors or subcontractors of Maimonides Health.
- Information Security: The Privacy Officer works with the Chief Information Security Officer and the Information System Department to ensure Maimonides Health's compliance with federal and state security regulations, including the HIPAA Security Rule and NYS Hospital Cybersecurity

Regulation, and the incorporation of relevant associated policies and procedures into the HIPAA compliance training programs.

- Marketing & Communications and Development departments: The Privacy Officer works with these departments to ensure that marketing and fundraising activities involving the use or disclosure of PHI comply with HIPAA, HITECH and Part 2 requirements.

B. WORKFORCE MEMBER TRAINING

The Privacy Officer and Office of Corporate Compliance helps ensure that Maimonides Health provides HIPAA training to all members of its workforce who have access to PHI/PII. The training provides an overview of Maimonides Health's privacy policies and procedures, including, but not limited to, a mandatory online HIPAA training course that Workforce Members must attend within thirty (30) days from the date of hire and at least, on an annual basis thereafter. Managers and supervisors are responsible for ensuring that Workforce Members who report to them attend orientation and annual mandatory training. Departments which retain non-employed professional staff (e.g., provided by outside agencies) are responsible for ensuring such personnel have received comparable training.

In addition to the training course referenced above, the Office of Corporate Compliance periodically issues privacy-related newsletters, posters and alerts and provides in-service education, as needed, to the Maimonides Health workforce.

The Privacy Officer, in collaboration with Senior Management, may also issue trainings in response to any privacy incidents that occur to help prevent any such incidents from occurring again and to ensure that Workforce Members are adequately educated. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce Maimonides Health's privacy policies and procedures.

C. INCIDENT RESPONSE TEAM

In the event a security incident results in the wrongful disclosure of PHI or PII, the Privacy Officer, in conjunction with the Incident Response Team, will take appropriate actions to prevent further inappropriate disclosures. The Incident Response Team is comprised of the Chief Compliance and Privacy Officer, the Chief Information Officer, the Chief Information Security Officer, a representative from the Office of Legal Affairs, and representatives from any other appropriate department deemed appropriate/ necessary to resolve the incident on an ad hoc basis in the reasonable judgement of the Privacy Officer. In addition, the Human Resources Department and the Office of Legal Affairs may be consulted and assist in the review and investigation of privacy incidents when required.

D. COMPLAINTS

Maimonides Health is committed to responding in a timely manner to any concerns or complaints about our privacy policies or procedures or compliance with applicable privacy laws. All Workforce Members are expected to follow Maimonides Health's established policies and procedures when Patients/ individuals make complaints regarding privacy issues.

- When a staff member receives a complaint, even if the complainant does not wish to file a complaint or provide identifying information, the staff member must notify the Office of Corporate Compliance by calling (718) 283-6608, visiting the Office of Corporate Compliance at 5402 Fort Hamilton Parkway, Brooklyn, NY 11219 (7th Floor), or by contacting the Compliance

Hotline (available 24 hours a day, seven days a week)at (800) 585-7970 or www.maimo.ethicspoint.com. Complaints may also be forwarded to the Patient Relations Department.

The Privacy Officer, or designee, will (i) investigate all such complaints promptly and determine who was involved in the possible privacy violation(s); (ii) recommend further action, if any, that should be taken, including but not limited to, sanctions to be applied against any Workforce Member or BA involved in such violation(s), (iii) document the results of such investigations, and (iv) to the extent necessary, in collaboration with the Office of Legal Affairs, report any such violations to the appropriate authorities or relevant federal, state or local agency.

ANY MEMBER OF MAIMONIDES HEALTH WORKFORCE WHO KNOWS OF OR SUSPECTS A VIOLATION OF HIPAA OR THIS PRIVACY POLICY AND ASSOCIATED POLICIES AND PROCEDURES MUST REPORT THE INCIDENT TO MAIMONIDES HEALTH'S PRIVACY OFFICER at 718-283-6608, Compliance@Maimo.org or via the 24/7 Compliance Hotline at (800) 585-7970 or www.maimo.ethicspoint.com.

V. ACCESS, USE AND DISCLOSURE OF PHI AND PII

As a general rule, pursuant to HIPAA and other privacy regulations, Maimonides Health employees or agents may only access, use or disclose PHI/PII/PI only as necessary to perform the duties within their scope of employment for legitimate business reasons. In practice, this means that no person covered by this Policy may access PHI/PII, or discuss or share PHI/PII, except for the purposes of Treatment, Payment, or Healthcare Operations, as discussed below, or as otherwise required or permitted by law.

Furthermore, any such access, use or disclosure of PHI must be limited to the **Minimum Necessary Standard** to accomplish the intended purpose or job function. When disclosing PHI, Maimonides Health takes reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. Similarly, when requesting PHI, Maimonides Health takes reasonable and appropriate steps to ensure that we only request the minimum amount of PHI necessary. This standard applies to oral, electronic, or paper communications involving PHI. Any questions concerning the application of this standard to requests or disclosures for PHI should be directed to the Privacy Officer and the Office of Legal Affairs, where appropriate, for review.

Prior to any PHI access, use or disclosure, Maimonides Health Workforce Members and BAs must ensure that the disclosure complies with this Policy, Maimonides Health's PHI use and disclosure procedures, and applicable laws. Maimonides Health Workforce Members and BAs are required to verify the identity of the individual requesting PHI and the authority of such individual to have access to the PHI, which may include obtaining documentation, statements or representations. Maimonides Health should only access, use or disclose PHI if acting on a good faith belief that the requesting individual's identity and authority has been verified.

Maimonides Health Workforce Members and BAs are prohibited from accessing Maimonides Health's Information Systems to view a Patient's medical record, the medical and/or demographic information of family members, friends, other staff members or individuals for personal or other non-work-related purposes, even if the Patient has given written or oral consent. Maimonides Health Workforce Members and BAs are also prohibited from accessing their own PHI through Maimonides Health's Information systems. To access this information, Workforce Members and BAs (even if they are Patients of

Maimonides Health) must follow the same procedures available to other Patients and not use their job-related access to access Maimonides Health's Information systems.

The following sections describe the conditions under which access, disclosure or use of PHI/PII/PI may be permissible.

A. PRIVATE INFORMATION (PI)

Maimonides Health collects, accesses, uses, and discloses Private Information for legitimate business, patient care, employment, operations, or legal purposes (e.g., insurance claims and payment processing, background checks, employment eligibility determinations, employee benefit enrollment, tax and legally required reporting).

Access to PI is limited to Workforce Members and approved third parties who have a legitimate and necessary business need to know the information and who are subject to appropriate confidentiality, contractual, privacy, and security obligations. Workforce Members must not access, use, disclose, copy, transmit, print, remove, or retain PI unless doing so is required for assigned responsibilities and consistent with this Policy and applicable procedures.

B. SOCIAL SECURITY NUMBERS (SSN)

Social Security Numbers must not be displayed on identification cards, badges, bulletin boards, public-facing materials, or in ay other manner visible to unauthorized persons. Documents, screens, reports, and other materials displaying SSNs must be kept out of public view and shown only to authorized Workforce Members or approved third parties.

SSNs may not be printed and mailed unless required by law or necessary for an application, enrollment, account, contract, policy, or verification process. When mailed, SSNs must not be visible through the envelope window or otherwise from outside the mailing.

SSNs may not be embedded or encoded on cards or documents, including through a barcode, chip, magnetic strip, or similar technology, unless reviewed and approved by Privacy, Information Security, and Legal Affairs. SSNs and other PI may not be transmitted over the internet or other unsecured channels unless the connection or transmission is secured or encrypted using an IS-approved method.

C. CREDIT AND DEBIT CARD INFORMATION

Cardholder data must be collected, processed, transmitted, stored, retained, and securely disposed of only as necessary to complete authorized business and payment processing activities, and in accordance with applicable payment card, privacy, security, and record retention requirements. Cardholder data must not be copied, stored, or retained outside approved payment systems or approved workflows unless specifically authorized and protected in accordance with the Payment Card Security Standard (PCI DSS).

Receipts and other payment records issued by Maimonides Health must not contain readily identifiable PII beyond what is needed for the transaction and may display no more than the last four digits of the Primary Account Number (PAN). Copies of receipts, forms, reports, or other records containing cardholder data or other Private Information must not be made or retained unless permitted under approved procedures.

D. ACCESS, USE AND DISCLOSURES OF PHI FOR WHICH AN AUTHORIZATION IS REQUIRED

Pursuant to HIPAA, Maimonides Health may disclose PHI pursuant to a completed **Authorization for the Use and Disclosure of Protected Health Information** form ("Authorization Form"). All uses and disclosures made pursuant to a signed Authorization Form must be consistent with the terms and conditions of the authorization. A Patient or their representative retains the right to revoke the authorization at any time, provided that such revocation is in writing and signed by either the Patient or their Personal Representative. The Authorization Form may not be combined with any other document to create a compound authorization, except that an authorization form created for a research study may be combined with another type of written permission for the same or another research study.

With respect to authorization, Maimonides Health must treat a Personal Representative as the Patient unless (i) the provider feels the individual being represented is a victim of abuse, neglect, and or domestic violence or (ii) the personal representative could endanger the individual (or in the case of a deceased Patient, conflicts with any prior expressed preference of the Patient). In either case, Maimonides Health may choose not to treat that person as the personal representative if in exercising professional judgment, doing so would be in the best interest of the individual.

i. Disclosures to Personal Representatives, Family, Friends or Others

There are instances when a Patient's family member, caregiver or friend may contact Maimonides Health to ask about a Patient, the Patient's status or whether the Patient has been seen at one of our medical offices. Unless the individual has been identified as the Patient's representative (e.g., HIPAA Personal Representative, guardian for health care purposes, parent/legal guardian of an unemancipated Minor Patient or other Qualified Person, health care agent or proxy designated in an advance directive, legal guardians of adults due to incapacity) within the Patient's medical record or the Patient has authorized the sharing of this information with the individual (e.g., caregiver), Maimonides Health staff should not release any Patient information.

In the case of an emergency, with input from the Administrator on duty, the minimum amount of PHI may be released in order to assist in resolving the emergency situation. Maimonides Health may use or disclose PHI to notify, or assist in the notification of (including identifying or locating a family member), a Personal Representative, or other person responsible for the care of the Patient of the Patient's location, general condition or death.

All disclosures to persons involved in the Patient's care or payment or for notification purposes must be made subject to the following requirements:

- When the Patient is present or otherwise available prior to the contemplated disclosure and has the capacity to make health care decisions, the disclosure may be made if the Workforce Member:
  - Obtains the Patient's agreement. It is best practice to affirmatively request permission from the Patient or ask that those present leave the room prior to disclosing information;
  - Provides the Patient with the opportunity to object to the disclosure, and the Patient does not express an objection; or
  - Reasonably infers from the circumstances, based on the exercise of professional judgement, that the Patient does not object to the disclosure.
- When the Patient is not present, lacks capacity or in an emergency circumstance, if:

- In the exercise of professional judgement, it is believed that the disclosure is in the best interests of the Patient; and
- Only PHI directly relevant to the person's involvement with the Patient's care or payment related to the Patient's health care or needed for notification purposes will be disclosed.

Any questions concerning whether a disclosure should be made in the situations described above should be directed to the Privacy Officer and, to the extent necessary, the Office of Legal Affairs.

ii. Disclosures Involving Sensitive Information

Sensitive information must be evaluated under both HIPAA and any more protective federal or New York State law before use or disclosure. Workforce Members shall not rely solely on general HIPAA TPO permissions where a more stringent law requires specific consent, patient authorization, court order, qualified protective order, or other heightened safeguards.

Maimonides Health requires specific authorizations for the use and/or disclosure of the following sensitive PHI, unless the Privacy Officer and Office of Legal Affairs have determined that there is a valid court order, subpoena, discovery request, warrant, summons or other lawful instructions from those courts or public bodies that require the disclosure:

- **Gender Identity and Sexual Orientation Information**

Information concerning gender identity, transgender status, sexual orientation, and related healthcare services shall be treated as confidential medical information and protected in accordance with HIPAA, applicable NY law, and Maimonides Health policies and procedures. Requests for this information that originate from outside Maimonides Health, including subpoenas, court orders, warrants, law enforcement requests, administrative inquiries, governmental requests, media inquiries, or requests from other third parties, shall be referred to HIS, the Privacy Officer, and/or the Office of Legal Affairs for review prior to any disclosure. Workforce Members shall not independently respond to such requests or release records without following established procedures.

- **Genetic information**

Information concerning the results of genetic tests, results of genetic testing of family members, information regarding an individual's or family member's request for or receipt of genetic services (e.g., genetic counseling), family medical history, or genetic information used to predict disease risk shall be used and disclosed in accordance with the federal Genetic Information Nondiscrimination Act ("GINA"), HIPAA, applicable NY law, and Maimonides Health policies and procedures.

- **HIV-related information**

Confidential HIV-related information shall be used and disclosed only in accordance with New York Public Health Law Article 27-F, including applicable HIV-specific authorization, disclosure, and redisclosure requirements. Disclosures of confidential HIV-related information must include any legally required notice prohibiting unauthorized redisclosure, unless an exception applies.

- **Mental health records**

Mental health information, including records protected by New York Mental Hygiene Law § 33.13 or other applicable law, shall be disclosed only to authorized persons or entities and only when the disclosure meets applicable legal requirements, clinical necessity, authorization, or court order standards.

- **Psychotherapy notes**

Psychotherapy notes are notes recorded by a mental health professional documenting or analyzing the contents of a counseling session and maintained separately from the Patient's medical record. Except as specifically permitted or required by law, Maimonides Health will not use of disclose psychotherapy notes without the Patient's written authorization.

- **Reproductive health information**

New York's reproductive-health "Shield Laws" limit cooperation with out-of-state investigations and legal proceedings related to lawful reproductive health services provided in New York. These protections extend to records and information concerning legally protected reproductive health activities.

Minor-consent and confidential services: Records relating to services for which a minor may consent under New York law, including certain reproductive health, pregnancy, abortion, contraception, emergency contraception, sexually transmitted infection, HIV, sexual assault, mental health, and substance use disorder services, must be handled to preserve the minor's applicable confidentiality rights. Parent, guardian, proxy portal, billing, and release-of-information access should be reviewed before disclosure.

- **Research**
- **Sexually transmitted diseases**
- **Substance Use Disorder (Alcohol and/or substance abuse) records**

Part 2 Records shall be used and disclosed only as permitted by 42 CFR Part 2. Disclosures made with patient consent must be accompanied by the required Part 2 notice and a copy of the consent or clear explanation of the scope of consent, and Part 2 Records may not be used or disclosed in civil, criminal, administrative, or legislative proceedings against the patient except as permitted by Part 2.

The following accesses, uses or disclosures of PHI do not require specific authorization:

- For public health purposes;
- For research purposes, if Maimonides Health receives only a cost-based fee to prepare and transmit the Patient information;
- For the sale, transfer, merger or consolidation of Maimonides Health; and,
- To a business associate, if Maimonides Health only receives remuneration for the performance of health care related activities.

iii. Disclosures for Marketing and Fundraising Activities

Pursuant to HIPAA, Maimonides Health requires patient authorization prior to the use and/or disclosure of PHI related to any of the following activities:

- Marketing activities involving direct or indirect remuneration to Maimonides Health for the PHI. If Maimonides Health, or Maimonides Health's BA, receives financial remuneration from a third party in exchange for Patient information, an authorization from the Patient is required including an acknowledgement that Maimonides Health will receive remuneration.

- Sale of PHI involving direct or indirect remuneration to Maimonides Health for the PHI.
  Marketing does not include the following as long as Maimonides Health does NOT receive financial remuneration in exchange for making the communication:

  - Refill reminders or other communications (e.g., availability of generics) concerning a drug or biologic that is currently being prescribed for the Patient so long as any financial remuneration received by Maimonides Health for making the communication is reasonably related to Maimonides Health's cost of making the communication (e.g., not more than the costs of labor, supplies, and postage);

  - Communication to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of Maimonides Health;

  - Communications for Treatment, including case management or care coordination, or to direct/recommend alternative treatments, providers, therapies, or setting of care.

  - Face-to-face communications with the Patient by Maimonides Health, its providers and/or workforce.

  - Promotional gifts of nominal value given to the Patient by Maimonides Health, its providers and/or workforce.

- Maimonides Health may use or disclose PHI to a BA for purposes of Outreach, provided that the PHI used is the minimum necessary to make the communication. If clinical information is used to make the Outreach communication, it must be limited to primary and secondary medical diagnoses. The Privacy Officer must approve all Outreach communications involving the use of clinical information.

  The Vice President of Marketing & Communications is responsible for establishing such controls as are necessary to ensure the consistent application concerning Marketing.

- Maimonides Health may use or disclose certain limited information for the purpose of contacting Patients to support its fundraising efforts, as long as each Fundraising communication provides the Patient with a clear and conspicuous opportunity to opt-out of any further fundraising communications without causing an undue burden on or more than a nominal cost to the Patient. The information used or disclosed for fundraising may include the Patient's name, address, phone number, email address, age, gender, date of birth, the dates Patient received treatment or services, the department of service, the name of the treating physician, outcome information, and health insurance status. Patients have the right to opt out of receiving any fundraising communications from Maimonides Health. A Patient's decision to opt out will not impact their treatment or payment for services. Maimonides Health may not make Fundraising communications to an individual where the individual has opted out of receiving such communication.

The Development Department must approve, in collaboration with the Privacy Officer and Office of Legal Affairs, to the extent necessary, all fundraising activities involving the use of PHI and/or PII.

iv. Use of Patient Information for Solicitation

Staff are prohibited from releasing Patient information for solicitation purposes. Patient names, addresses, and telephone numbers are considered confidential and must be handled with the highest level of privacy. This prohibition includes, but is not limited to, sharing patient information with diaper services, photographers, life insurance companies, or similar entities.

v. Media Access to PHI

Patient authorization is required prior to permitting media, including film crews, to access areas of Maimonides Health where PHI may be accessible. Simply masking (such as blurring or pixelating) patients' faces, voices, or other PHI during publication is not sufficient as the PHI is initially disclosed to the media crew itself, not the public. Written authorization is required even if Workforce Members do the filming or capturing of information in another format, and then provide it to the media or public. Special care should be taken as PHI may be inadvertently disclosed via patient information displayed on doors or in patient rooms, notes on bulletin boards, data on clinical monitors or even a patient's presence in a particular area within Maimonides Health. Maimonides Health will take reasonable safeguards such a computer privacy screens, opaque barriers, and chaperoning the media crew or otherwise subjecting them to reasonable oversight while they are on the premises.

Maimonides Health will first obtain at least an oral consent from the Patient to allow Maimonides Health to disclose the Patient's identity to Marketing & Communications Department. The Marketing & Communications Department may then contact the Patient about the story and request written authorization.

Where Maimonides Health hires a media company to create training videos and PHI is involved, a BAA should be signed, and Patient authorizations obtained as necessary.

vi. Disclosures of PHI for Deceased Persons

Maimonides Health must comply with the requirements of HIPAA with respect to the PHI of a deceased Patient for a period of 50 years following the death of the Patient. During this time, PHI may be disclosed to:

- Personal Representatives: Individuals authorized under state law to act on behalf of the deceased patient.
- Family Members or Close Friends: If the disclosure is relevant to the individual's involvement in the deceased's care or payment for care prior to death, and the patient did not object during their lifetime.

After 50 years from the date of death, PHI is no longer protected under HIPAA, and the information is considered de-identified and may be used or disclosed without restriction.

vii. Prohibition on Photography or Recording by Patients, Family Members, Visitors and Other Third Parties

To ensure compliance with HIPAA and other applicable laws—and to support the delivery of high-quality care while safeguarding privacy—Maimonides Health takes reasonable steps to protect patients, visitors, and staff from unauthorized photography, video or audio recording, and other forms of image capture. This includes preventing the inadvertent recording of PHI/PII through surveillance or personal devices.

To protect patient privacy:

- Patients, family members, and visitors are not permitted to photograph or record:
  - Other patients (under any circumstance)
  - Maimonides Health personnel, equipment, or facilities (e.g., Emergency Department)
  - Themselves or their own family member receiving care—unless consent is obtained from Maimonides staff
- Any such activity must be explicitly authorized by Maimonides staff and in accordance with this Policy and relevant procedures.

If a patient, visitor, or third party is recording or photographing in violation of the above:

1. Provide them with a copy of this policy.
2. Politely ask them to stop the unauthorized activity.
3. If they refuse:
   - Ask them to leave the premises.
   - Contact **Patient Relations to assist with enforcement** if they decline to leave.
   - If still noncompliant, contact **Security to escort the individual off premises**.
   - If refusal continues after intervention by Security, **law enforcement** should be contacted.

Staff should never delay, withhold, or deny medical treatment to a Patient due to violations of this Policy.

This Policy does **not limit** the applicability of **Medical Center Policy AD 141 Virtual Visitation (Remote Communication)**. That policy continues to apply in appropriate circumstances to support remote communication and virtual visitation.

E. ACCESS, USE, AND DISCLOSURE OF PHI FOR WHICH AUTHORIZATION IS NOT REQUIRED

Maimonides Health may access, use and disclose PHI without an individual authorization as set forth below. Any questions concerning the appropriate access, use or disclosure of PHI without an individual authorization should be directed to the Privacy Officer and Office of Legal Affairs, to the extent necessary.

i. Treatment, Payment and Healthcare Operations (TPO)

Maimonides Health may use and disclose PHI, without an individual's authorization, for TPO purposes. Maimonides Health may disclose PHI to another covered entity without individual authorization for these purposes to the extent that the other covered entity has or had a relationship with the Patient and the PHI pertains to that relationship.

RHIO / SHIN-NY / Healthix

Where Maimonides Health participates in a RHIO, QE, Healthix, or the SHIN-NY, participation and disclosures shall comply with 10 NYCRR Part 300, applicable SHIN-NY policy guidance, participation agreements, patient consent requirements, and applicable federal and state privacy laws.

Maimonides Health may contribute patient information to a QE/RHIO as permitted by law and applicable participation agreements. Access to or retrieval of patient information through the QE/RHIO by Maimonides Health Workforce Members shall occur only for authorized purposes, through approved systems, by authorized users, and consistent with patient consent status and applicable exceptions.

Maimonides Health shall maintain or rely on appropriate audit controls to monitor access to patient information through the QE/RHIO and shall investigate suspected inappropriate access, use, or disclosure in accordance with this Policy and applicable incident response procedures.

Special categories of information, including minor-consent information, HIV-related information, mental health information, genetic information, and Part 2 Records, must be handled in accordance with applicable federal and New York State law and SHIN-NY policy requirements.

ii. Disclosures of PHI to Business Associates (BA)

Staff may disclose PHI to vendors or subcontractors identified as Maimonides Health's BA and/ or BA subcontractor and allow them to create, transmit, maintain, process, or receive PHI on Maimonides Health's behalf. However, Maimonides Health must first obtain assurances from the BA that it will appropriately safeguard the information through a Business Associate Agreement ("BAA"). BAAs clarify and limit, as appropriate, the permissible uses and disclosures of PHI by the BA, based on the relationship between the parties and the activities or services being performed by the BA. Prior to allowing a BA access to Maimonides Health's PHI, Maimonides Health must execute an underlying agreement for services and a BAA (or addendum) with the BA. No BAA submitted from an outside organization is authorized for signature unless and until expressly reviewed and approved by the Office of Legal Affairs. The Privacy Officer is the authorized signatory for BAAs.

All managers who have authority to negotiate and/or enter into vendor contracts are responsible for contacting the Office of Legal Affairs when evaluating the vendor's scope of work in order to determine whether a BAA is required and for preparing/negotiating BAAs.

When it is determined that a BAA is required as part of the vendor contract, the department where the services are being rendered will be responsible to provide the following information to Procurement, Information Systems ("IS"), or Legal Affairs, as applicable, depending on the nature of the service:

- The BA's name and contact information and Maimonides business owner/end user/requestor of services;
- Description of services being provided by the BA; and
- Type of PHI to be created, maintained, received or processed by the BA, and how the PHI is being handled or stored by the BA.

If applicable, Information Services will evaluate the BA's technical security controls and safeguards prior to entering into a BAA. Furthermore, BAs will be subject to information security reviews as indicated by IS security standard operating procedures, and if applicable, will be required to bind all subcontractors

that use or disclose Maimonides Health PHI to the same restrictions and conditions regarding PHI as are applicable to the BA.

Maimonides Health may use or disclose PHI to a BA for purposes of Outreach, provided that the PHI used is the minimum necessary to make the communication. If clinical information is used to make the Outreach communication, it must be limited to primary and secondary medical diagnoses. The Privacy Officer must approve all Outreach communications involving the use of clinical information.

Before sharing any PHI with outside consultants or contractors who meet the definition of a Business Associate, staff must verify with their department supervisor that a BAA is in place. Inquiries concerning BAAs may be directed to the owner of the contract, the Office of Legal Affairs, or the Privacy Officer.

iii. Disclosures of Limited Data Sets (LDS)

To the extent practicable, Maimonides Health may use or a disclose a LDS of information without a patient's authorization provided certain conditions are met. First, the purpose of the disclosure may only be for research, public health or health care operations. Second, the recipient of the LDS must enter into a data use agreement with Maimonides Health that establishes the permitted uses and disclosures of the limited data set. In order for health information to be considered a LDS, the following identifiers must be removed:

- names;
- street addresses (other than town, city, state and zip code);
- telephone numbers;
- fax numbers;
- e-mail addresses;
- Social Security numbers;
- medical records numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate license numbers;
- vehicle identifiers and serial numbers, including license plates;
- device identifiers and serial numbers;
- URLs;
- IP address numbers;
- biometric identifiers (including finger and voice prints); and
- full face photos (or comparable images).

The health information that may remain in the information disclosed includes:

- dates such as admission, discharge, service, DOB, DOD;
- city, state, five digit or more zip code; and
- ages in years, months or days or hours.

The remaining information constitutes PHI, and remains subject to the requirements of HIPAA.

iv. Disclosures of De-Identified Information

Maimonides Health may freely use and disclose information that has been "de-identified" in accordance with the HIPAA Privacy Rule. De-identified information is PHI that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

Individually identifiable health information may be de-identified in either of two ways:

- Statistical method
- Safe Harbor method where, pursuant to HIPAA, 18 Patient identifiers and those of the Patient's relatives, employers, or household members are all removed.

v. Facility Directories

Maimonides Health may use or disclose limited information about a Patient within its Facility directory after giving the Patient an opportunity to agree or object. The information may include: the Patient's name, the Patient's location in the hospital (e.g., room number); the Patient's condition (described in general terms that do not communicate specific medical information about the Patient), and the Patient's religious affiliation to members of the clergy.

If the Patient objects to some or all of the information being included in the Facility directory, Maimonides Health must comply with the Patient's objection. If the opportunity to agree or object cannot be provided because of the Patient's incapacity or emergency treatment circumstance, Maimonides Health may use or disclose limited PHI for the Facility directory, if such disclosure is consistent with the prior expressed preference of the Patient, if any, that is known to Maimonides Health and is in the best interest of the Patient in the exercise of professional judgement. Maimonides Health must thereafter inform the Patient and provide the opportunity to agree or object when it becomes possible to do so. Information about Patients in behavioral health departments will not be included in the Facility directory.

vi. Disclosures of Employee Records and Protected Information

Employee records (e.g., employee health services records, credentialing files) and Human Resources materials containing PHI or PII are strictly confidential and must be securely stored within the Human Resources Department ("HR") with restricted access. These files may not be removed from HR without written authorization from either the Senior Vice President or the Vice President of Human Resources.

Accessing an employee's personal medical information, such as reviewing hospital records to verify sick leave, doctor's appointments, or work-related injuries, is strictly prohibited. Additionally, using personal medical information in employment-related decisions is not allowed.

vii. Other Permissible Disclosures of PHI without Authorization:

When specific requirements are satisfied, Maimonides Health may disclose PHI in the following situations without the Patient's authorization:

- About victims of abuse, neglect or domestic violence;
- For judicial and administrative proceedings;
- For law enforcement purposes;
- For public health activities;
- For health oversight activities;

- About decedents;
- For cadaveric organ-, eye- or tissue-donation purposes;
- For certain limited research purposes;
- To avert a serious threat to health or safety;
- For specialized government functions; and
- That relate to workers' compensation programs.

The Privacy Officer and, to the extent necessary, Office of Legal Affairs, should be involved in determining whether PHI may be disclosed for any of the situations described above.

F. MITIGATION OF INADVERTENT DISCLOSURES OF PHI/PII

Maimonides Health shall mitigate, to the extent practicable, any harmful effects that become known to it from a use or disclosure of an individual's PHI/PII in violation of HIPAA or Maimonides Health's privacy/security policies and procedures and applicable laws. A Workforce Member, BA or BA subcontractor must immediately contact the Privacy Officer once they become aware of an unauthorized use or disclosure of PHI/PII, so that Maimonides Health can take appropriate steps to mitigate harm to the Patient.

Workforce Members must immediately report any lost, stolen, or suspected compromised data, paper files, remote devices, laptops, portable media, credentials, or other materials that contain or may contain PHI/PII or Private Information to their manager, the Privacy Officer, and Information Security. Managers receiving such reports must promptly escalate them to the Privacy Officer and Information Security for assessment and response.

G. SECURING, TRANSMITTING, RETAINING & DESTROYING PHI/PII

i. Safeguards and Firewalls

Maimonides Health has established administrative, technical, and physical safeguards to prevent PHI/PII and Private Information from intentionally or unintentionally being accessed, used, or disclosed, retained, transmitted, or disposed of in violation of HIPAA, New York law, and Maimonides Health requirements.

- Administrative safeguards include avoiding any action that might provide PHI/PII to an unauthorized individual or agency and refraining from reviewing or accessing records or files without a legitimate business need or without authorization.
- Technical safeguards include limiting access to information by creating computer firewalls. Firewalls ensure that only authorized staff will have access to PHI/PII, that they will have access to only the minimum amount of PHI necessary for their job functions, and that they will not further use or disclose PHI in violation of the HIPAA Privacy Rule. Additionally, all staff can only access PHI/PII using their own login information. Maimonides Health has implemented security policies that set forth the security measures in place to protect the privacy of PHI/PII.
- Physical safeguards include taking reasonable precautions so that PHI/PII is not visible or audible to passers-by, retrieving documents containing PHI/PII from printers upon printing; locking doors or filing cabinets, periodically changing door access codes and use of staff identification badges, placing in locked shred bins or otherwise destroying labels, documents, disks or any other media containing PHI/PII prior to disposal.

Department managers are responsible for making access requests for staff under their supervision. This includes updating or revoking access as staff responsibilities change.

New York Hospital Cybersecurity and Access Governance (10 NYCRR § 405.46)

Maimonides Health shall maintain cybersecurity safeguards, policies, procedures, governance, access controls, audit trails, incident response processes, vulnerability management, third-party risk management, and training consistent with New York hospital cybersecurity requirements and applicable Information Security policies.

Access to systems containing PHI/PII shall be based on role, job function, and minimum necessary principles; shall be reviewed periodically; and shall be modified or terminated promptly when workforce role, employment, contract, or business need changes.

Cybersecurity events or incidents involving PHI/PII, electronic health records, patient care systems, medical devices, third-party systems, ransomware, or material operational disruption must be escalated promptly to Information Security, Privacy, Legal Affairs, and other required stakeholders for assessment of reporting obligations under HIPAA, the SHIELD Act, 10 NYCRR § 405.46, and other applicable laws.

ii. Electronic Health Records

Maimonides Health has implemented electronic health record systems (the "Systems") which, like paper records, must comply with the HIPAA requirements, as well as other state and federal laws and regulations. The Systems are encrypted and security parameters are set so that only authorized staff and BAs can access and/or view PHI/PII. The Systems also provide an electronic tracking system that provides an accounting history of when records have been accessed and who accessed them. PHI which is part of the medical record should not be saved outside of the Systems, including to a computer desktop, flash drive or mobile device.

iii. AI and Ambient Clinical Documentation Controls

Workforce Members may not enter, upload, dictate, paste, summarize, or otherwise disclose PHI/PIII into public, consumer-grade, or unapproved AI tools, chatbots, transcription services, summarization tools, or other automated technologies.

Approved AI or ambient clinical documentation tools may be used only in accordance with approved workflows, vendor agreements, privacy/security reviews, patient notice or consent requirements, and clinical documentation standards. Use of such tools must not replace professional judgment, required clinical review, or provider responsibility for the accuracy and completeness of the medical record.

AI tools used for patient care decision support, triage, risk scoring, diagnosis, treatment recommendations, scheduling prioritization, or other patient-impacting functions must be reviewed before implementation and periodically thereafter for potential bias, discriminatory impact, transparency, clinical validity, and appropriate human oversight. Such approved AI tools must be used only in accordance with approved clinical, privacy, security, legal, and operational workflows and must not replace professional judgment or provider responsibility for patient care decisions.

AI tools that create or support documentation, triage, clinical decision support, coding, billing, scheduling, patient engagement, quality, compliance, or operational functions involving PHI/PII must include appropriate safeguards, including role-based access, audit logging, data minimization, retention/deletion controls, vendor/subcontractor restrictions, and human oversight.

iv. Mailing/ Faxing/Texting

Where the HIPAA Privacy Rule allows Maimonides Health to share PHI with another organization, provider or with the Patient, Maimonides Health may use a variety of means to deliver the information, as long as it uses reasonable safeguards to protect the Patient information from inappropriate use or disclosure to unauthorized persons. These safeguards will vary depending on the mode of communication used. For example:

- When mailing Patient information, check to verify that the name and address of the recipient are correct and current, that the contents relate to the recipient and the address on the envelope (mailing label) matches the address of the recipient.
- When faxing Patient information, always verify the recipient's fax number before sending, double check the fax number to ensure accuracy, and include a completed fax cover sheet with every transmission.

Tampering with incoming or outgoing Maimonides Health 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 to be opened only by the addressee.

It is prohibited to use cell service provider text messaging (SMS or MMS) to transmit patient data between caregivers, unless the technology has been approved by IS.

v. Online Tracking, Website, Mobile App, and Digital Communications Controls

Maimonides Health shall not deploy or materially modify tracking technologies on websites, patient portals, mobile applications, scheduling platforms, donation pages, marketing pages, email campaigns, or other digital properties that may collect or disclose PHI/PII without prior Privacy, IS, Legal Affairs, and Marketing/Communications review, as applicable.

The review shall determine whether the technology collects or transmits individually identifiable information, health-related information, appointment information, portal activity, IP address, device identifiers, cookies, advertising identifiers, URLs, search terms, or other data that may constitute PHI/PII when connected to a patient or health care interaction.

Tracking technologies may not disclose PHI/PII to third parties unless the disclosure is permitted by law, consistent with patient notice/authorization requirements, supported by a BAA or other required agreement where applicable, and approved through the applicable privacy and security review process.

Text messaging, email, chat, patient engagement, and mobile communication tools must be approved by IS and Privacy before use with PHI/PII and should include safeguards such as encryption, access controls, authentication, message minimization, retention controls, opt-out management, and identity verification where appropriate.

vi. Removing PHI/PII from Maimonides Health's Premises

Although Maimonides Health may deem it necessary for an employee to work from a location other than one of its sites (e.g., medical office, corporate site), it is still required to reasonably safeguard that PHI/PII from unintentional disclosure to unauthorized persons.

Every Workforce Member is required to:

- Reasonably safeguard PH/PII from any intentional or unintentional use or disclosure that is a violation of HIPAA and/or other privacy regulations; and
- Reasonably safeguard PHI/PII to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Unless expressly authorized by Maimonides Health's Senior Management, sending, transmitting, or otherwise disseminating or disclosing proprietary data, trade secrets or other confidential information, including medical records and/or Patient data is prohibited. Therefore, PHI/PII may only be accessed and/or removed under the following circumstances:

- Prior to removing PHI from a Maimonides Health site for a legitimate business reason, approval must be received from Senior Management. Additionally, if the information is ePHI, approval from the Office of Information Security is also required.
- Maimonides Health will provide encrypted laptop computers for employees required to work offsite and access PHI/PII in a non-Maimonides setting. Any files saved on these computers should be saved to the network and not locally. Documents stored this way are secured and protected from unauthorized disclosure as well as loss or destruction (e.g., from theft or damage to the laptop).
- Medical Staff and Maimonides Health staff must not transmit PHI/PII over the Internet or other unsecured networks, unless using a secure encryption procedure as authorized by IS.
- The electronic removal of PHI/PII (e.g., using flash drives or other devices) for purposes of working from a non-Maimonides setting is generally prohibited. In the very rare circumstances that such electronic removal may be necessary, prior approval of the Chief Information Security Officer and Privacy Officer is required.
- Maimonides Health's remote portal allows staff to securely access applications, websites (internal websites such as the Intranet or Sharepoint) and file shares (H: drive, I: drive, etc.). Staff are not to print ePHI (e.g., from SCM, other application containing ePHI) that is available remotely. The use of personal email accounts for sending and receiving email communications related to Maimonides Health business is prohibited.
- In the limited circumstances that the paper (e.g., Patient records, reports) removal of PHI/PII is necessary, the paper must be transported in a secure, locked carrying case.
- The following safeguards concerning PHI/PII are required of all staff when working from a non-Maimonides Health site:
    - Only work on PHI/PII in a secure, private environment.
    - Keep the information with you at all times while in transit.
    - Do not permit others to have access to the information (e.g., leaving documents in personal vehicle used by family members).
    - Never email Patient or other sensitive information unless logged into Maimonides Health.
    - Don't save PHI/PII on your personal computer.
    - Do not print records of any type.
    - Do not record login information on or near the computer.
    - Return all information the next business day or as soon as required.

Upon termination of employment, termination of contract with Maimonides Health, or revocation of authorization to access PHI/PII, medical and Maimonides Health staff members must return any and all copies of PHI/PII in their possession or under their control to Maimonides Health.

The Privacy Officer will immediately investigate any incident that involves the loss or theft of PHI/PII that was taken off-site.

vii. Disposal of PHI/PII

PHI/PII and Private Information may be disposed of only by means that ensure the information cannot be read, reconstructed, re-identified, or further disclosed to an outside party. Each Workforce Member granted access to PHI/PII or Private Information must ensure that any documents labels, files, devices, or electronic media containing PHI/PII have been secured or destroyed in accordance with this Policy and associated Maimonides Health policies and procedures. PHI/PII shall not be discarded in unsecured or open trash bins, unsecured recycle bags or other publicly accessible locations. Only secure containers for disposal of any paper documents containing PHI/PII will be used prior to destruction. Documents containing PHI/PII may only be destroyed by incineration or shredding. Shredders and/or secure containers (i.e., vendor provided HIPAA bins) are located throughout Maimonides Health facilities. Electronic media, systems, devices, and other technology assets containing PHI/PII or Private Information must be disposed of in a manner that renders the information unreadable or unrecoverable and complies with IS policies and procedures. Departments should consult IS before disposing of electronic media or systems that may store PHI/PII or Private Information.

VI. PATIENTS' HIPAA RIGHTS

A. NOTICE OF PRIVACY PRACTICES

The Privacy Officer is responsible for developing and maintaining a notice of Maimonides Health's privacy practices (NPP) that describes (i) the uses and disclosures of PHI that may be made by Maimonides Health, (ii) the Patients' individual rights, and (iii) Maimonides Health's duties with respect to the PHI.

Maimonides Health posts the NPP on its website and at its medical offices and other locations (i.e., designated reception areas).

Maimonides Health provides the NPP to all Patients (or their representatives) at the time of registration and upon request. In an emergency situation, Maimonides Health will provide the NPP to the Patient, or the Patient's Personal Representative, as soon as reasonably practicable after the emergency treatment.

Maimonides Health makes a good faith effort to obtain the Patient's, or Personal Representative's signature acknowledging receipt of the NPP. If a signed Acknowledgement is not obtained, staff shall document their efforts to obtain such acknowledgement and the reason why it was not obtained (e.g., individual refused to sign) in the space provided.

Maimonides Health incorporates the completed and signed NPPs into the Patient's medical record.

Each Department involved in the activities listed above is responsible for instituting appropriate procedures to ensure that these requirements are met. Site practice administrators, Ambulatory Health Services Network directors, and Patient Relations are responsible for helping to ensure compliance. Maimonides Health will take reasonable steps, based upon identified language needs, to translate and provide the NPP to Patients with limited English proficiency.

B. ACCESS TO PROTECTED HEALTH INFORMATION

Patients have the legal right under HIPAA and NYS Public Health Law § 18 to inspect and obtain copies of their PHI and certain other medical records maintained by Maimonides Health or its BAs. Requests for access to medical records, billing records, or other records (whether or not they contain PHI) should be directed to the Privacy Officer or the Health Information Services ("HIS") Department. Maimonides Health will process requests in accordance with applicable federal and New York State requirements, including verification of the requestor's authority, applicable response timeframes, fees, and any limitations on access permitted by law. Special rules may apply to certain categories of information, including mental health, HIV-related, and Part 2 substance use disorder treatment records.

Requests to access, exchange, or use electronic health information shall also be reviewed for compliance with the Information Blocking regulations (45 CFR Part 171). Workforce Members shall not adopt blanket delays, manual workarounds, suppression rules, portal release restrictions, or denial practices that are likely to interfere with legally permissible access, exchange, or use of electronic health information unless an applicable legal requirement or Information Blocking exception supports the practice and the rationale is documented.

C. REQUESTS TO AMENDMENT

HIPAA also allows Patients to request that Maimonides Health amend PHI contained in their medical records. Maimonides will consider requests for amendment that are submitted in writing by the Patient on Maimonides Health's **Request to Amend** form. HIS will forward the request to amend to the provider who created the information or, alternatively the provider designated by the Chair to review the PHI in the absence of the treating provider.

Maimonides Health may deny a Patient's request for any of the following reasons:

- The request is not in writing;
- The request did not explain why the Patient believes Maimonides Health should make the amendment;
- The PHI or record that is subject to the request was not created by Maimonides Health;
- The PHI or record is not part of the Designated Record Set;
- The PHI or record is not available for inspection relating to the Patient's right to access his/her PHI; or
- The PHI is accurate and complete.

In the event the request is accepted, the appropriate administrative department (e.g., HIS, Revenue Cycle) and/or BA will be responsible for amending the record accordingly.

The HIS Department will respond to the requests to amend within 60 days from the date Maimonides Health received the request. If the amendment is denied in whole or in part, HIS will provide the Patient with a written denial that will include: (i) the basis for the denial, (ii) a statement of the Patient's right to submit a written statement disagreement with the denial and how the Patient may file such a statement; (iii) a statement that if the Patient does not submit a statement of disagreement, the Patient may request that Maimonides Health provide the Patient's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and (iv) a description of how the Patient may submit a complaint to Maimonides Health or the Office of Civil Rights. HIS will prepare a written rebuttal to the Patient's statement of disagreement and provide a copy to the Patient.

In the event that IS cannot respond within 60 days, HIS must notify the Patient in writing explaining the reason for a 30-day extension and the date by which Maimonides Health will respond.

The HIS department will use all reasonable efforts to forward the amendment to (i) persons or organizations that the Patient has stated should be notified; and (ii) any person or organization who may have relied, or may rely in the future, on the original information is a way that may negatively affect the Patient. Any future disclosures of the Patient's PHI must include the amended information. HIS will, as appropriate, append or otherwise link the Patient's request to amend, Maimonides Health's acceptance or denial of the request, the Patient's statement of disagreement, if any, and Maimonides Health's rebuttal, if any, to the Designated Record Set.

If Maimonides Health is informed by another Covered Entity (e.g., healthcare provider or health plan) of an amendment to a Patient's PHI, HIS will amend the PHI in the Designated Record Set as provided. HIS is responsible for ensuring that the PHI is amended as required.

D. ACCOUNTING OF DISCLOSURES

Maimonides Health is required to keep records of certain disclosures of a Patient's PHI to third parties and to provide an accounting of those disclosures for the prior six years to Patients who request such an accounting. All accounting of disclosure inquires will be directed to the Privacy Officer and HIS Department. The HIS Department, with assistance of the relevant authorized staff, processes requests for an accounting of disclosures upon receipt of a completed **Request for Accounting of Disclosures** form. Maimonides Health must provide the accounting within 60 days of the request. A one-time extension of an additional 30 days will be allowed if the requestor is notified in writing as to the reason for the delay and the date by which the accounting will be provided. The first accounting to a Patient in any 12-month period shall be without charge.

The accounting provided for the Patient must be in writing and must include the following information for each disclosure:

- Date;
- Name (and address, if known) of the recipient of the disclosure;
- Brief description of the PHI disclosed;
- Brief statement of the purpose of the disclosure or a copy of the written request for disclosure (if any);
- If multiple disclosures of PHI have been made to the same person or organization for the same purpose (other than for the excepted disclosures), then only the accounting for the first disclosure must include the information noted above;
- In the case of multiple disclosure accounting, the frequency and number of disclosures, date range of the accounting period and the date of the last disclosure must also be included.

Because a Patient may request an accounting of disclosures at any time, staff must record, on an ongoing basis, all information that is needed to respond to a Patient's request regarding disclosures of information. Certain information must be recorded about each disclosure: the date of the disclosure; the recipient of the PHI and the address of the recipient, if known; a description of the information disclosed; and a statement of the purpose of the disclosure or a copy of the written request leading to the disclosure. The authorized staff who disclose a Patient's PHI without the Patient's written authorization MUST maintain a retrievable accounting either in the Patient's medical records and/or in other administrative methods.

Types of Disclosures Which Must Be Recorded

- For public health activities (e.g., for vital statistics, disease control reporting, etc.)
- For FDA regulated products or activities;
- For purposes of reporting abuse (child abuse, neglect, others as required by state law);
- For healthcare oversight activities (e.g., to an agency for investigations, licensure and disciplinary actions, etc.);
- For judicial and administrative proceedings (e.g., in response to a court order);
- For law enforcement purposes (e.g., reporting gunshot wounds, for identification purposes);
- Regarding victims of a crime
- Regarding the reporting of a crime on the premises;
- Regarding the reporting of a crime in emergencies;
- For the provision of information to coroners, medical examiners, and funeral directors.
- Third-party requests allowable by law that do not require Patient Authorization;
- Federal and/or state inquiries required by law (e.g., CMS or Department of Health);
- For organ, eye, or tissue donation purposes;
- For research purposes (see below for special accounting rules apply in research context);
- In order to avert a serious threat to health of safety;
- For military/veterans activities (e.g., for armed forces personnel to assure proper execution of a military mission);
- For workers compensation purposes;
- Disclosures to or by BAs for any of the above purposes;
- Disclosures made without authorization.

Tracking Disclosures for Research

Any Disclosures of PHI/PII made without the written authorization of the research subject must be tracked. This includes studies conducted under a waiver of authorization, as well as situation where authorization was obtained but the recipient of the PHI/PII is not listed on the authorization form. When a Limited Data Set is used, there is no requirement to track the disclosure.

A modified tracking mechanism is available for research involving the disclosure of PHI from 50 or more subjects (i.e., during epidemiological research). Under a modified tracking mechanism, the researcher must be prepared to provide:

- The name and description of all protocols involving disclosure of 50 or more subjects;
- A brief description of the types of PHI disclosed;
- The dates or time periods of the disclosures;
- Contact information of the recipients;
- A statement that a specific individual's PHI may or may not have been disclosed for a particular study;
- If multiple disclosures of PHI have been made to the same person or organization for the same purpose (other than for the excepted disclosures), then only the accounting for the first disclosure must include the information noted above;
- In the case of multiple disclosure accounting, the frequency and number of disclosures, date range of the accounting period and date of the last disclosure must also be included.

Types of Disclosures Which Do Not Have To Be Recorded

- Sharing PHI with staff and the treating health care providers;
- Disclosures for Maimonides Health to carry out TPO activities (including disclosures to BAs or members of the Organized Health Care Arrangement (OHCA) such as medical staff, Maimonides Midwood Community Hospital);
- Disclosures made pursuant to the Patient's specific written authorization;
- Disclosures to the Patient or the Patient's Personal Representative;
- Disclosures that are incidental (e.g., statements in a waiting room that may have been overheard);
- Disclosures made for national security and intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials without authorization, with custody of the Patient;
- Disclosures made as part of a Limited Data Set;
- The information has been de-identified;
- Facility directory information;
- If the Patient has agreed to suspend the right to an accounting;
- Disclosures that occurred more than six years from the date of the request for accounting; and
- Disclosures that occurred prior to April 14, 2003.

The same general guidelines provided by state law for copying of records will be applied for each additional account during the same 12-month period. If a charge will be made, the individual must be notified in advance and given the opportunity to retract or limit the request in order to avoid or reduce the charge.

Law enforcement or health oversight agencies can request a suspension of the accounting of disclosures to that agency. Such requests can be written or verbal. If the request is written, it must specify the time period and reason for the suspension. If the request is verbal, suspension is limited to 30 days unless the agency submits a written statement that states an accounting will be reasonably likely to impede the agency's activities and specifies how long the suspension will be in force. Employees contacted by law enforcement will notify the Office of Legal Affairs.

E. REQUESTS FOR ALTERNATIVE COMMUNICATION MEANS OR LOCATION

From time to time, Patients may request certain additional privacy protections for their PHI. For example, Patients may request that we communicate with them by an alternative means or method (e.g., different contact number, use of patient portal) that is more confidential for them. They may also request that we communicate with them at alternative locations (e.g., alternative mailing address, temporary address, alternative or private phone number).

Under HIPAA, special procedures must be followed when handling such requests. Patients requesting additional privacy protections should therefore be directed to submit their written requests on completed **Patient Request for Confidential Communications** form directly to the Office of Corporate Compliance, or the Administrator at the medical office site and/or the HIS Department who will forward the request to the Privacy Officer. Completed requests may be honored if, in the sole discretion of Maimonides Health, the requests are deemed to be reasonable.

The HIS Department will prominently place in the Patient's medical record a notice explaining how all Maimonides Health staff and medical staff members should communicate with the Patient. The notice must be sent to Patient Accounts, the Admitting Office, the Ambulatory Health Services Network Administrative Office, Patient Relations Department, the MIS Department and the Psychiatry Medical Records Room. If the Patient is a Minor, the notice must also be sent to the Administrator, Pediatric department. All staff are expected to review a Patient's medical record for possible restrictions on how and/ or where we communicate PHI with the Patient.

Patient portal access, proxy access, caregiver access, and electronic release of test results or visit information must be configured and monitored to protect confidential communications, minor-consent services, sensitive information, and restrictions requested by the patient or required by law.

Proxy access for parents, guardians, caregivers, health care agents, or other representatives shall be granted, limited, modified, or revoked based on verified authority, patient preference where applicable, minor-consent confidentiality requirements, and applicable federal and New York State law.

Where disclosure through the portal could reveal confidential minor-consent services, HIV-related information, Part 2 Records, mental health information, reproductive health information, domestic violence-related information, or other sensitive information, operational procedures should address appropriate segmentation, suppression, redirection to MIS review, or other safeguards.

F. REQUESTS FOR RESTRICTION ON USES AND DISCLOSURES OF PHI

A Patient may request in writing restrictions on the use and disclosure of his/ her PHI by submitting the **Patient Request for Restrictions or Limitations on Access, Use, or Disclosure of Protected Health Information** form to the Office of Corporate Compliance. For all Patients, the Office of Corporate Compliance will consult with the HIS department in addition to the practice manager/supervisor and/or affected hospital operational department(s) to determine whether the request will be granted or denied and to ensure that the request can be met. It is Maimonides Health's policy to attempt to honor such requests, if in the sole discretion of Maimonides Health, the requests are reasonable and otherwise permitted by law. Maimonides Health may deny any request that is not a required restriction. Depending on the circumstances, exceptions to the Patient's ability to restrict access, use or disclosures of their PHI may include psychotherapy notes, information compiled for use in civil, criminal, or administrative actions, and information that is subject to prohibition by the Clinical Laboratory Improvements Amendments.

The Patient will be notified in writing by the HIS Department whether the request has been granted or denied. Documentation of the restriction must be sent to Patient Accounts, the Admitting Office, the Ambulatory Health Services Network Administrative Office, Maimonides Health Outpatient Cardiology Center, the MIS Department and the Psychiatry Medical Records Room as applicable. If the Patient is a Minor, the documentation of the restriction must also be sent to the Administrator, Pediatric department. Applicable departmental personnel will properly flag the encounters in the Patient's medical records. All Workforce Members are expected to review a Patient's medical record for possible restrictions on the use and disclosure of the Patient's PHI.

Maimonides Health may initiate a modification to or terminate a restriction if the Patient agrees to or requests the termination in writing at any time by submitting the **Written Request/Agreement to Terminate Requested Restrictions** form. A Maimonides Health Workforce Member documenting a Patient's oral requests on the designated form is considered sufficient to meet this writing requirement.

All other oral requests will be deemed insufficient. For restrictions agreed upon, Maimonides Health may terminate its restriction if the use and disclosure are necessary for emergency treatment and Maimonides Health requests that the recipient health care provider not further use or disclose the information. Maimonides Health also may terminate its agreement to a restriction if it informs the Patient in writing. All modifications and/or the termination of a restriction, whether initiated by the Patient or Maimonides Health, are only effective with respect to PHI created or received after the Patient either makes the request or has been informed of the termination.

i. Restricting Disclosures to a Health Plan

Maimonides must agree to a Patient's restriction on the disclosure of the Patient's PHI to the Patient's health plan if the disclosure is for the purpose of carrying out payment or health care operations, is not otherwise required by law, the Patient (or other person other than the health plan on behalf of the Patient) has paid Maimonides Health in full for health care services provided, and the PHI involved pertains solely to such health care services. Maimonides Health will not violate this restriction, except to the extent that such a use or disclosure is required by law or the restriction has been properly terminated:

- The Patient revoked the restriction in writing, or
- The Patient defaulted on the payment(s) for services covered by the restriction.

The Patient will be required to complete the **Request to Restrict Disclosure Acknowledgement** form.

- This form should be thoroughly discussed and submitted to Patient Registration or Admitting (or the appropriate practice manager for outpatient visits).
- The health care item or service is flagged with the appropriate payor type (e.g., Self-pay).
- Payment in full or the estimated payment must be made on the date of service.
- The completed form is scanned into the Patient's medical record.

By requesting this type of disclosure restriction to a Health Plan, the Patient understands that:

- All estimated costs must be paid based on the standard self-pay discounted rate on the date of the service,
- The final bill must be paid in full when received or a payment plan is in place in coordination with financial counseling,
- They are not eligible for financial assistance beyond a payment plan as described here,
- Only those records relating to the fully paid out-of-pocket services will be kept from the Health Plan, and
- They will not submit any bills for the included services to the Health Plan.

If a Patient defaults (i.e., fails to pay) on payment(s), Maimonides Health has the right to bill and disclose the information necessary to obtain payment from the Health Plan, after reasonable efforts have been made to collect payment. The Patient will be responsible for payment of the full amount due for all services not covered by the Health Plan, including those not covered because pre-authorization was not obtained prior to the service and the timeline for submission to the Health Plan has lapsed due to Maimonides Health providing the Patient opportunity to submit payment.

The Patient is responsible for alerting or requesting restrictions with all other providers not listed on the form.

G. REQUESTS FOR A COPY OF THE PATIENT'S MEDICAL RECORD

A Patient may request a copy of his/her medical record by completing a HIPAA compliant Authorization (release of information) Form and submitting it to the HIS department. These requests will be processed in a timely fashion and forwarded pursuant to the authorization. Sensitive information may not be released unless appropriately requested within the authorization.

Requests from Minors ordinarily require consent of parent, guardian, or legal representative unless:

- The Minor is an Emancipated Minor.
- Relates to treatment related to Emancipated Minor's child.
- Concerns health services related to reproductive care including:
    - Family planning
    - Emergency Contraception
    - Abortion
    - Pregnancy/prenatal care
    - Sexually transmitted diseases
    - Sexual assault

i. When the Requestor is the Patient

Maimonides Health will take reasonable steps and exercise professional judgment to verify the identity of the individual making a request for access to his/her own PHI. This includes requesting government issued photo identification (e.g., driver's license) and verifying it matches the image previously scanned into the Patient's medical record when requests are made in-person. If the request is made over the telephone, verification will be accomplished by requesting identifying information (i.e., requesting minimum two Patient identifiers). Requests in writing must be made on a HIPAA compliant Authorization Form. Maimonides Health may verify the validity of the authorization by contacting the Patient.

ii. When the Requestor is the Patient's Personal Representative or other Qualified Person

Maimonides Health will take reasonable steps and exercise professional judgment to verify the identity of the individual making a request for access to a Patient's PHI. For in-person requests, this includes requesting government issued photo identification (e.g., driver's license) to establish identity. Authority to make such a request will be verified by confirming the person is named in the Patient's medical record (e.g., is identified in the Patient's profile as the Patient's legally authorized representative) and/ or a valid authorization (e.g., completed HIPAA Personal Representative form, Health Care Proxy, Guardianship or other court ordered appointment, Power of Attorney for health care purposes) is in the Patient's medical record. For initial requests, a copy of the government issued photo identification and legal notice must be attached to the request and placed in the Patient's medical record.

H. FILING A PATIENT COMPLAINT RELATED TO PHI ACCESS, USE OR DISCLOSURE

Patients may file complaints related to Maimonides Health's access, use or disclosure of PHI to the Office of Civil Rights in writing by mail to the Centralized Case Management Operations, U.S.

Department of Health and Human Services, 200 Independence Avenue, S.W. Room 509F HHH Bldg., Washington, D.C. 20201, email at OCRCompliant@hhs.org, by calling their toll-free number 1-800-368-1019, TDD 1-800-537-7697, or online at https://www.hhs.gov/hipaa/filing-a-complaint/index.html. Patients may also contact the New York State Department of Health via email at hospinfo@health.state.ny.us, mail to NYS DOH Centralized Hospital Intake Program, Bureau of Hospital and Primary Care Services, Mailstop/CA/DCS, Empire State Plaza, Albany, NY 12237, by calling toll-free number 1-800-804-5447

Maimonides Health shall not retaliate in any for against any patient who files a complaint in good faith. Maimonides Health will never, as a condition of the provision of treatment, require Patients to waive their rights under the privacy regulations, including, without limitation, the right to file a complaint to the U.S. Department of Health and Human Services or to the Privacy Officer concerning possible privacy violations.

VII. BREACH REPORTING

Maimonides Health actively strives to prevent Breaches of unsecured PHI or Security Breaches of Private Information. In the event such a Breach occurs, federal and state laws require Maimonides Health to comply with certain reporting, documentation and investigation requirements of known or suspected action(s) or adverse event(s) resulting from unauthorized use or disclosure of PHI/PII/Private Information. A Breach shall be treated as discovered by Maimonides Health or a BA of Maimonides Health as of the first day on which such Breach is known to Maimonides Health or BA or, by exercising reasonable diligence, would have been known to Maimonides Health or BA.

To the extent applicable and required by law, Maimonides will notify affected individuals, HHS, the media, and state agencies if a Breach of unsecured PHI or a Security Breach of Private Information occurred as soon as possible and in no case later than 60 days from discovering the Breach.

To determine whether a Breach has occurred, applicable law requires Maimonides Health to demonstrate there is a low probability that the PHI/PII has been compromised based on a risk assessment of the following factors:

- The nature and extent of the PHI/PII involved;
- The unauthorized person who used the PHI/PII or to whom the disclosure was made:
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI/PII has been mitigated.

The term Breach does not include:

- Any unintentional acquisition, access, or use of PHI/PII by a Maimonides Health Workforce Member or individual acting under the authority of a Maimonides Health facility or BA if:
  o Such acquisition, access, or use was made in good faith and within the course and scope of authority; and
  o Such information is not further used or disclosed in a manner not permitted; or
- Any inadvertent disclosure of PHI/PII by a person who is authorized to access PHI/PII at a Maimonides Health facility or BA if the information is not further used or disclosed impermissibly; or

- A disclosure of PHI/PII where a Maimonides Health facility or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- Under SHIELD Act, notification may not be required where the exposure was an inadvertent disclosure by persons authorized to access the information and Maimonides Health determines that the exposure is not likely to result in misuse of the information, financial harm to the affected persons, or emotional harm in the case of unknown disclosure of online credentials. The Office of Corporate Compliance, in consultation with IS and Legal Affairs as appropriate, will document and retain the determination and make any required regulatory reports.

In all cases, the Office of Corporate Compliance must be contacted to make the determination of whether or not a breach has occurred.

A. BREACH NOTIFICATION REQUIREMENTS

If an individual becomes aware of a Breach of Unsecured PHI or a Security Breach of Private Information, they must notify the Office of Corporate Compliance immediately. If a Business Associate becomes aware of a Breach of Unsecured PHI or a Security Breach of Private Information, they must notify Maimonides Health without unreasonable delay (within 10 days of discovery) per the terms of the BAA.

Breach analyses shall consider all potentially applicable federal and state notification requirements, including HIPAA/HITECH, the New York SHIELD Act, New York Department of Health requirements, 10 NYCRR § 405.46 cybersecurity incident reporting requirements, 42 CFR Part 2 breach reporting obligations, contractual reporting requirements, and the laws of states where affected individuals reside.

Where a cybersecurity incident may materially affect hospital operations, patient care systems, electronic health records, or other information systems, IS shall coordinate with Privacy, Legal Affairs, and operations to determine whether notice to the New York State Department of Health or other governmental entities is required and to preserve incident evidence, logs, and documentation.

Following a Breach of Unsecured PHI, Maimonides Health must provide notification of the Breach to the affected individual if necessary and in certain circumstances, to the media (if the Breach affects more than 500 Patients).

- Individual Notice to affected Patients must be written in plain language and sent by first-class mail to the last known address of the Patient or the next of kin, or alternatively, by encrypted email if the affected individual has agreed to receive such notices electronically. If the Patient is deceased, the next of kin or Personal Representative shall be notified. If the Patient is incapacitated/incompetent, the Personal Representative shall be notified. If the Patient is a Minor, the parent or guardian shall be notified unless otherwise required by law.
- If Maimonides Health has insufficient or out-of-date contact information for 10 or more individuals, Maimonides Health must provide substitute individual notice by either conspicuously posting for 90 days the notice on the homepage of its web site or by providing the notice in major print or broadcast media where the affected individual likely resides. The Office of Corporate Compliance will work directly with the Public Relations department or its designee in arranging for this notification.

- When fewer than 10 individuals are affected, Maimonides Health may provide substitute notice by an alternative form of written, telephone or other means.
- These notices must be provided without unreasonable delay and in no case later than 60 days following the discovery of a Breach. The notice must include, to the extent possible, a description of the Breach, a description of the types of information that were involved in the Breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what Maimonides Health is doing to investigate the Breach, mitigate the harm, and prevent further Breaches, as well as contact information for Maimonides Health and a toll-free number for individuals to contact Maimonides Health to determine if their PHI was involved in the Breach.
- Media Notice to a prominent media outlet serving the State or jurisdiction is required if Maimonides Health experiences a Breach of Unsecured PHI affecting more than 500 Patients. These notices must be provided without unreasonable delay and in no case later than 60 days following the discovery of a Breach and include the same information required for the Individual Notice. The Office of Corporate Compliance will work directly with the Public Relations department or its designee in arranging for this notification.
- The Office of Corporate Compliance shall provide notice to HHS concerning Breaches of Unsecured PHI. If a Breach affects 500 or more individuals, Maimonides Health must notify HHS without unreasonable delay and in no case later than 60 days following the discovery of a Breach. If a Breach affects less than 500 individuals, Maimonides Health may use the electronic form available on the HHS website and submit no later than 60 days after the end of the calendar year in which the Breach occurred. Maimonides Health shall also provide notification to the New York State Attorney General of any breach reported to the Secretary within five business days of notifying the Secretary, regardless of whether the breach includes Private Information.
- Notification by a BA of a Breach of Unsecured PHI or Security Breach of Private Information must be provided to Maimonides Health without unreasonable delay (within 10 days of discovery) and per the terms of the BAA. To the extent possible, the BA will provide Maimonides Health with the identification of each Patient affected by the Breach as well as any information required to be provided by Maimonides Health in its notification to the affected Patients.
- Notification to the individual may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the notification will be made after law enforcement determines it will not compromise its investigation.
- State Law analysis of the requirements for notification of the particular State in which the Patients reside will be conducted and documented.

If a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed by up to 30 days, if the statement is made orally. Such oral statement should be documented and include the identity of the official making the statement. If the statement is in writing and specifies the time for which a delay is required, such notification, note or posting shall be delayed for the time period specified by the official.

B. SECURITY BREACH OF PRIVATE INFORMATION

Under the New York State SHIELD Act, any Breach of the security of Maimonides computerized data involving the Private Information of a New York State resident, where such information has been accessed, acquired, or is reasonably believed to have been, accessed/acquired without valid authorization and that compromises the security, confidentiality or integrity of the Private Information must be assessed to determine whether notification is required to affected individual(s) and required governmental, regulatory, or law enforcement agencies. For New York residents, required notice may include notice to the NYS Department of Health, NYS Attorney General, the NYS Department of State Division of Consumer Protection, NYS Department of Financial Services, NYS Division of State Police, and other agencies as applicable. Such notices shall comply with applicable requirements regarding the timing, content, and distribution of notices and the approximate number of affected individuals. If Maimonides Health determines that disclosure of Private Information of over 500 New York State residents is not a breach under the SHIELD Act, Maimonides Health shall provide the written determination to the New York State Attorney General within five days of the determination.

In the event that more than 5,000 New York residents are to be notified at one time, the Marketing & Communications Department shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected persons as appropriate.

In the event of a Security Breach or similar action involving Patients in states other than New York, the Office of Corporate Compliance will work with the Office of Legal Affairs to take the necessary steps to notify the Patient(s) and other out of state governmental or regulatory agencies accordingly.

VIII. SANCTIONS FOR VIOLATIONS OF MAIMONIDES HEALTH'S PRIVACY POLICIES, PROCEDURES AND APPLICABLE LAW

Sanctions for accessing, using or disclosing PHI/PII in violation of HIPAA or this Policy will be imposed in accordance with Maimonides Health's policies and procedures and contingent on the degree and severity of the violation. The Privacy Officer, in consultation with Human Resources, are responsible for reviewing and recommending appropriate sanctions for substantiated failures to comply with this Policy. Violations involving non-employed members of the Medical Staff will be reviewed by the Privacy Officer and the President of the Medical Staff. Violation determinations will be forwarded by the President of the Medical Staff to the Executive Medical Council for appropriate action.

Violations of this Policy will be subject to disciplinary action based on the facts and circumstances surrounding the policy violation. Intentional or reckless behavior for misconduct will be subject to more significant disciplinary action as outlined in the Human Resources policies and procedures. Applicable contractors, agents, subcontractors, and independent contractors' disciplinary procedures are governed by their contracts. Disciplinary procedures for non-employed members of the Medical Staff are governed by the applicable Medical Staff Bylaws, Rules and Regulations. Maimonides Health Board members' disciplinary procedures are governed by the Maimonides Health Board of Trustees By-laws.

Level 1 violation is considered to be minor and unintentional. These types of violations are not considered a direct threat to privacy, as they usually do not include the intent to further access, use or disclose the information or use the information to harm the Patient whose PHI/PII has been compromised.

- Accidental use or misuse of information;

- Carelessness/ a lack of privacy awareness education;
- Fails to protect information in a reasonable manner that results in an inadvertent disclosure.

Maimonides Health's response to a Level-1 violation may include verbal warning and mandatory re-education for a first offense. A repeated incident from the same person requires more stringent disciplinary action, up to, and including termination.

Level 2 violation occurs when there is an intentional disregard of an established privacy and/ or information security policy or procedure.

- The user is aware of the privacy/ security policies and procedures, but is willing to circumvent them in order to achieve a personal goal.
- Fails to log off of a session, terminal or application when left unattended;
- Assessing information without utilizing the proper documented procedure such as viewing Patient information without authorization or by knowingly using a workstation logged on with another user's credential to access Patient information.
- Assessing information that would not normally be accessed in the normal course of job responsibilities such as accessing birthdates, addresses of friends/ relatives/colleagues, or accessing records out of curiosity.
- Collecting information on any Patient or sets of Patients without permission and outside the scope of his/her job responsibilities.
- Releasing records or information in an inappropriate manner.
- Discussing Patient information in public areas without discretion thereby allowing visitors/ workers that would not be authorized to access this information to overhear the discussions.
- Accessing Patient information on behalf of another user that would not normally have access under normal circumstances.
- FairWarning violations

Maimonides Health's response to a Level-2 violation may include, but not be limited to, a minimum of a written reprimand with retraining on HIPAA policies and procedures, probation, suspension, or termination.

Level 3 violations include intentional actions of any user when accessing, reviewing, disclosing, or discussing PHI/PII for personal gain, or with malicious intent. These types of incidents are considered the most serious and must be dealt with accordingly. It could cause personal damage to some party, and fines and/or civil action against Maimonides Health as well as to the violator.

- Intentionally releasing personal, corporate, or medical information for personal gain or profit.
- Collecting information such as Patient lists or mailing addresses for personal gain or profits.
- Intentionally destroying or altering any information with intent to harm.
- Releasing information of any individual with the intent to cause harm or adverse publicity, or for personal gain or profits.
- Intentionally attempting to bypass security controls and attempting to gain unauthorized access to PHI/PII.

Maimonides Health's response to a Level-3 violation may include, but not be limited to suspension without pay or termination of employment/contract or other engagement, possible civil penalties and/ or criminal prosecution.

IX. NO INTIMIDATING OR RETALIATORY ACTS; NO WAIVER OF HIPAA PRIVACY

Maimonides Health prohibits any intimidation, threats, coercion, discriminate against, or any retaliatory action against any individual for exercising their HIPAA related rights, filing a complaint, participating in an investigation, or opposing any acts the individual believes in good faith violate Maimonides Health policies and procedures, HIPAA or applicable privacy related regulations.

X. DOCUMENTATION RETENTION

Maimonides Health's privacy policies and procedures shall be documented and maintained for at least six (6) years from the date last in effect.

This Policy supersedes the following policies: *HIPAA 001- Notice of Privacy Medical Centers; HIPAA-002 Business Associates; HIPAA-004 Patient Requests to Amend Protected Health Information; HIPAA-005 Confidential Communications; HIPAA-006 Request for Restrictions on the Use and Disclosure of PHI; HIPAA-007 Uses of Protected Health Information in Accordance with the Minimum Necessary Standard; HIPAA-009 Receiving and resolving Compliant regarding Privacy of Protected Health Information; HIPAA-010 Patient Requests for Accounting of Disclosures; HIPAA-011 Sanctioning of Employees, agents and contractors for HIPAA violations; HIPAA-013 Training of Work Force on HIPAA requirements ; HIPAA-014 Notification of Breach of Unsecured PHI; HIPAA-015 Marketing and Sale of Protected Health information; HIPAA-016; Photography of Record by Patients, Family Members, Visitors, and Other Third Parties; AD-124 Confidentiality of PHI for Patients and Employees; AD-048 Release of Confidential Information for Purpose of Solicitation, and AD-135 Protection of Private Information.*

REFERENCES**:**

Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 160 & 164
HIPAA Privacy Rule 45 CFR Part 164, Subpart E
HIPAA Security Rule 45 CFR Part 164, Subpart C
HIPAA Breach Notification Rule 45 CFR § 164.402
Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of American Recovery and Reinvestment Act of 2009 (ARRA), Pub.L.111-5 (Feb.1, 2009)
42 CFR Part 2 Substance Use Disorder Records
10 NYCRR § 405.46 Hospital Cybersecurity Requirements
NY GBL § 899-aa Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)
NY HIV Confidentiality (Article 27-F)
NY Mental Hygiene Law § 33.13 for mental health confidentiality requirements
NY Public Health Law § 18 for medical records access by patients

New York City Human Rights Law, N.Y.C. Admin. Code § 8-102(23)
AD-065 Implementation of Patients' Rights and Patients' Responsibilities
AD-141 Virtual Visitation (Remote Communication)
COMPL-021 Identity Theft Prevention and Detection Program
HIPAA SEC-003 Management of Access to Electronic Protected Health Information
HIPAA SEC-011 Physical Security of the Medical Center's Workstations, Devices & Electronic Media
HIPAA SEC-017 Removal and/or Transportation of Protected Health Information Outside the Medical Center
INFO SYSTEMS-009 Remote Access
INFO TECH-014 Mobile Device and Portable Media
INFO TECH-017 MMC IT Access Authorization and Management
MARCOMM-003 Media Guidelines
MED RCDS-005 Release of Medical Information from the Patient's Record
MED RCDS-009 Release of Behavioral Health Patient's Medical Records to External Agencies
MED RCDS-019 Destruction of Patient Health Information
MED RCDS-026 Designated Record Set and Legal Health Record
RES-019 Use and Disclosure of Protected Health Information for Research Purposes

INDEX: HIPAA, Privacy, Breach, marketing, fundraising, patient rights, PHI, business associate

RESPONSIBLE DEPARTMENT: Corporate Compliance