MAIMONIDES MEDICAL CENTER

CODE: HIPAA– 011 (Reissued)
DATE: April 13, 2017
ORIGINALLY ISSUED: September 22, 2005

RE: SANCTIONING OF EMPLOYEES, AGENTS, AND CONTRACTORS FOR HIPAA VIOLATIONS

I POLICY

Maimonides Medical Center has established and will apply appropriate sanctions against members of its workforce, as well as agents and contractors, who fail to comply with its policies and procedures. This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to sanctioning for violating the Medical Center's policies and procedures. Under the Health Insurance Portability and Accountability Act, penalties for misuse or misappropriation of health information include both civil monetary penalties and criminal penalties. Civil penalties range from $100 to $50,000 for each violation to a maximum of $1,500,000 per year for the same violation. Criminal penalties vary from $50,000 and/or 1 year imprisonment to $250,000 and/or 10 years imprisonment (42 USC§§ 1320d-5 and 1320d-6).

II RESPONSIBILITY

A. All Medical Center workforce members must comply with HIPAA's privacy and security regulation requirements.

B. Sanctions for violations will be recommended by the Privacy Officer and, in the case of violations involving EPHI (electronic protected health information) the Security Officer. The individual's Department Head and the Vice President for Human Resources must concur in the imposition of the sanction.

III PROCEDURE

A. The Medical Center will apply appropriate sanctions against members of its workforce who fail to comply with the Medical Center's policies and procedures.

B. The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors.

C. Employees, agents, and other contractors should be aware that certain violations may require or result in notification to law enforcement officials as well as regulatory, accreditation, and/or licensure organizations.

D. The policy and procedures contained herein do not apply specifically when members of the Medical Center's workforce exercise their right to:

1) file a complaint with HHS;

2) testify, assist, or participate in an investigation, compliance review, proceeding, or hearing related to enforcement of HIPAA; or

3) oppose any act made unlawful by the HIPAA privacy or security rule; provided the individual or person has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA privacy or security rule;

4) disclose protected health information as a whistleblower and the disclosure is to a health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individuals legal options with regard to the whistleblower activity; or

5) an employee who is a victim of a crime and discloses protected health information to a law enforcement official, provided that the protected health information is about a suspected perpetrator of the criminal act.

E. The Medical Center has divided violations of patient confidentiality into three levels with the corresponding disciplinary action for each level of violation.

Level 1. Carelessness

This level of violation occurs when an employee unintentionally or carelessly accesses, reviews or reveals patient information to him/herself or others in a manner not permitted under HIPAA without a legitimate need to know the patient information. Examples include, but are not limited to: employees discuss patient information in a public area; employee leaves patient health information in a public area; employee leaves a computer unattended in an accessible area with protected health information unsecured.

Disciplinary Sanctions. Depending upon the facts, counseling, oral warning, written warning, final written warning or suspension, documented in writing and maintained in the employee's personnel record, or termination. Except in the case of termination, the employee shall be

required to review the confidentiality policies (HIPAA-7 "Uses of Protected Health Information in Accordance with the Minimum Necessary Standard" and AD-124 "Confidentiality of Protected Health Information for Patients and Employees")

Level 1 Disciplinary Sanctions. Repeat offenders of level I offenses will be subject to progressive discipline, up to and including termination, per HR-12

Level 2. Curiosity or Concern (no personal gain)

This level of violation occurs when an employee intentionally accesses or discloses patient information in a manner not permitted under HIPAA for purposes other than the care of the patient or other authorized purposes but for reasons unrelated to personal gain. Examples include, but are not limited to: an employee looks up birth dates, address of friends or relatives; an employee accesses and reviews a record of a patient out of concern or curiosity; an employee reviews a public personality record.

Disciplinary Sanctions:
Depending upon the facts and circumstance a minimum of a written warning, up to a maximum of termination, per HR-28, HR-11.

Except in the case of termination, the employee shall be required to review the Confidentiality Policy

Level 3. Personal Gain or Malice.

This level of violation occurs when an employee accesses, reviews, or discusses patient information in a manner not permitted under HIPAA for personal gain or with malicious intent. Examples include but are not limited to: an employee reviews a patient record to use information in a personal relationship; an employee compiles a mailing list for personal use or to be sold.

Disciplinary Sanctions: Termination, per HR 28

F. The actual disciplinary action will be recommended by the Privacy Officer after investigation and decided by the individual's supervisor in conjunction with Human Resources.

G. Violations involving non-employed members of the Medical Staff will be reviewed by the Privacy Officer and the President of the Medical Staff. If a determination is made that a violation of this policy has occurred, the President of the Medical Staff shall refer the matter for appropriate action by

the Executive Medical Council. If investigation by the Executive Medical Council results in a finding that improper conduct took place, the physician shall be disciplined in accordance with the Medical Staff By-Laws.

H. Independent contractors and vendors who violate the privacy and security regulations of HIPAA may be subject to termination of contract. Such situations shall be reviewed by Privacy Officer with the applicable Department Head of the area responsible for retaining the contractor or vendor.

I. In addition to the sanctions outlined in this policy, civil or criminal penalties may apply.

J. Documentation concerning sanctions imposed pursuant to this policy will be retained for a period of at least 6 years from the date of the imposition of the sanction.

IV **CONTROL**

A. The Privacy Officer and the Security Officer will monitor compliance with this policy.

B. The Compliance Officer will receive information regarding sanctions imposed.

_____

Kenneth Gibbs
President & CEO

INDEX:	Sanctions, Disciplinary Action
REFERENCES:	Security Rule §164.306 (68FR8377); HITECH §13410 (d) (effective February 19, 2009) 74 FR 56123, Interim Final Rule (October 30, 2009)
ORIGINATING DEPARTMENT:	Legal Department