Status **Active** PolicyStat ID **14319491**

Origination	12/1/2011	Owner	Elise Lipoff Mayer: Director of Operations
Last Approved	9/6/2023	Area	Foundation
Effective	9/6/2023		
Last Revised	9/6/2023		
Next Review	9/5/2025		

Privacy and Security of Donor Information, FSec01

I. POLICY:

It is the policy of the Mount Sinai Medical Center Foundation to preserve the trust and confidence of donors, to comply with applicable law, and to safeguard the resources of the Medical Center through appropriate measures to safeguard personal information pertaining to donors, prospects and others.

II. PURPOSE:

To ensure that all Fundraising Staff employed by, or associated with, the Mount Sinai Medical Center Foundation take appropriate steps to ensure the security, confidentiality and privacy of donor information for the protection of our donors and patients.

III. DEFINITIONS:

As used herein, "Fundraising Staff" means all Mount Sinai Medical Center Foundation employees. "Donor" means any actual or potential donor or prospect for whom the Mount Sinai Medical Center has individually identifiable information, such as name, address, phone number, email, etc. "Donor Information" includes all information about a Donor which is created, used, stored or transmitted by or on behalf of the Mount Sinai Medical Center Foundation. "Donor Information" includes information in both "hard copy" and electronic form (e.g. information supplied to or obtained from Raiser's Edge®, Salesforce®, Epic® and similar databases and electronic records).

IV. PROCEDURE:

A. **Privacy of Donor Information**

1. It is the responsibility of all members of the Fundraising Staff to ensure the privacy of Donor information. To this end, each member of the fundraising staff shall

observe the following safeguards:

a. Conversations with Donors, prospects, and family members which may involve confidential or sensitive information must be held in locations, and under circumstances, which ensure privacy. Donor information must not be discussed in public areas or with unauthorized individuals.

b. No Donor information, including sensitive information such as name(s), addresses, phone number, email, financial information, medical information and the like may be disclosed to any person except with the full knowledge and consent of the individual providing the information. The use or disclosure of health information pertaining to any Donor, potential donor or other person shall occur only as permitted by applicable law, including the obtaining of an authorization when and as required by the HIPAA Privacy Rule, 45 CFR §§ 160 and 164.

c. Donor information will not be sold, traded or shared with any other entity.

B. **Security of Donor Information**

1. It is the responsibility of all members of the Fundraising Staff to secure all Donor Information at all times. To this end, each member of the Fundraising staff shall observe at least the following safeguards:

a. **Printed or Hard Copy Donor Information**:

i. Any Donor information in printed or hard copy form including pledge cards or financial information (i.e. credit card, debit card, checking account number with routing numbers) shall be processed within 48 hours. Once this Donor information has been processed, the information must be placed in the shredding bin. Any pledge cards or financial information not processed during and after 48 hours, must be kept in the safe or locked drawer within the Foundation office. The Director of Operations and/or designee (i.e. Senior Accountant) is the only individual that will have access to the safe. All printed and hard copy financial information that does not require storage must be placed in the shredding bin for destruction within the same business day. Removal of Donor information from the foundation office is not allowed, unless prior approval is obtained from the Chief Development Officer/Vice President - Foundation for legitimate business reasons.

ii. On a daily basis, each member of the fundraising staff shall review all printed or hard copy Donor information in his/her possession, and securely destroy (e.g., shredding bin) any such information which is no longer needed for legitimate purposes of the Mount Sinai Medical Center Foundation.

b. **Electronic Donor Information**: Access by Fundraising Staff to electronically-stored Donor information is limited to individuals authorized by the Chief Development Officer/Vice President - Foundation or designee. Each such individual shall observe the following safeguards:

i. Access to electronically-stored Donor information is limited to workstations within the Foundation Office as well as Medical Center supplied laptops unless otherwise approved by the Chief Development Officer/Vice President - Foundation.

ii. Passwords and other logon information may not be shared with any person for any reason.

iii. Users shall log off any computer system with access to Donor information when not in use, and at the end of each working shift.

iv. Display terminals which exhibit Donor information must be positioned so as to prevent viewing by unauthorized individuals.

v. Electronically-stored Donor information including emails and text messages may not be copied, printed or saved except as is reasonably necessary for legitimate business purposes of the Mount Sinai Medical Center Foundation. Any Donor financial information (i.e. credit card, debit card, checking account number with routing numbers) in electronic format including text messages shall be processed within 48 hours. Once this Donor information has been processed, this information must be deleted immediately from your email or phone.

vi. E-mailing, transmitting, or otherwise disseminating any electronically-stored Donor information is not permitted without the express approval of the Chief Development Officer/Vice President - Foundation or designee. Any such e-mailing, transmission or dissemination must be encrypted and comply with applicable law, including but not limited to the requirements of the HIPAA Security Rule, 45 CFR §§ 160 and 164.

vii. Accessing, using, or storing electronically-stored Donor information via portable electronic devices or storage media (e.g. Smartphone, PDA, USB memory device) shall follow the same rules as for a workstation or company-supplied laptop.

C. **Enforcement**: Any failure to comply with the requirements of this policy may subject the offender to disciplinary action, up to an including termination of employment. Violations of this policy may also subject the offender to civil and/or criminal penalties under applicable law.

V. REFERENCES:

Health Insurance Portability and Accountability Act 45 CFR §§ 160 and 164.
HIPAA Omnibus Final Rules (January 17, 2013).
MSMC Foundation Policy 2.30.044 ("Fundraising and HIPAA Requirements").
Association of Fundraising Professionals "*Code of Ethical Principles and Standards*" (Standard Number 10) (2007).

Approval Signatures

Step Description	Approver	Date
	Summary Sklar	9/6/2023
	Elise Lipoff Mayer: Director of Operations	9/6/2023