Planned Parenthood
Care. No matter what.
Planned Parenthood of Metropolitan Washington, DC

Donor and HIPAA Privacy Policies

POLICY STATEMENT:

Planned Parenthood of Metropolitan Washington, DC conducts fundraising programs. It is the policy of Planned Parenthood of Metropolitan Washington, DC to maintain appropriate privacy safeguards to ensure the confidentiality and information security of donors.

SCOPE: This policy applies to all Planned Parenthood of Metropolitan Washington, DC workforce members.

PROCEDURES: Actions to Be Taken

1. The HIPAA Privacy and Security Officials are responsible for ensuring donor privacy and data security.
2. The Privacy and Security Officials working with development or the fundraising department have identified the types of donor data that is received, stored, used or disclosed.
3. The Privacy Official has identified the use of PHI for fundraising and educated the fundraising managers on the opt- out requirements with each fundraising campaign or communication.
4. The Privacy Official has determined that the fundraising manager and team maintains a functional process to allow for opt-out of fundraising campaigns and a methodology to ensure that opt-out requests are promptly recorded and adhered to.
5. The Privacy Official shall oversee all PHI sorting/selection for fundraising campaigns to ensure that minimum necessary restrictions are adhered to.
6. If a business associate is used to manage fundraising activities, the Privacy Official will ensure a valid business associate agreement is in place that identifies the specific permitted uses of PHI, including those used to identify patients for potential targeted fundraising.
7. If an Institutionally related foundation handles fundraising for this organization, they shall be identified as such and allowed disclosures of PHI as it pertains to fundraising.
8. The Privacy Official shall ensure the PHI used or disclosed to a business associate or institutionally related foundation is limited to:

    (i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

    (ii) Dates of health care provided to an individual;

    (iii) Department of service information;

    (iv) Treating physician;

    (v) Outcome information; and

(vi) Health insurance status.

9. The Privacy Official will review every fundraising communication to ensure that the proper opt-out language is in place as well as the following practices adhered to including:

   "(i) A statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice of privacy practices.

   (ii) With each fundraising communication made to an individual a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

   (iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

   (iv) A covered entity may not make fundraising communications to an individual where the individual has elected not to receive such communications under paragraph (f)(1)(ii)(B) of this section.

   (v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications."

   – Taken from 45CFR § 164.520(b)(1)(iii)(B)

10. Periodically, the Privacy Official shall review the opt-out process and communications to ensure that it remains in place and functional.

11. Donor information will never be sold or exchanged without proper donor authorization.

12. Donor financial information will be protected according to PCI best practices including the masking of credit card numbers and the encryption of all bank account information.

13. Donor information is considered personally identifiable information; the HIPAA safeguards have been evaluated to represent the equivalent or greater level of data security than State regulations.

14. Any unauthorized access or disclosure of unsecured personally identifiable donor information is treated as a potential State data breach; the Privacy Official shall investigate and follow all required notification and reporting requirements. 45 CFR §165.514(f)