



HIPAA and Fundraising

FUNDRAISING ACTIVITY INCLUSION

Preamble 65 FR 82491 Health care operations include business management activities and general administrative functions, including:

- Fundraising for the benefit of the covered entity (CE) to the extent permitted under **164.514**;
- **65 FR 82546** "Institutionally related foundation" means a foundation that:
 - Qualifies as a non-profit foundation under 501(c) (3) of IRS code
 - Has in its charter statement of charitable purposes an explicit linkage to the CE
- **65 FR 82718** Permissible fundraising activities include appeals for money, sponsorship of events etc...(but) do not include royalties or remittances for the sale of products to third parties.

INFORMATION/DATA USAGE

§164.514(f)(1) A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following PHI for the purpose of raising funds for its own benefit, without authorization

- Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;
- Dates of health care provided to an individual;
- Department of service information;
- Treating physician(s);
- Outcome information;
- Health insurance status

NOTIFICATION

- **§164.520(b) (1) (iii) (B)** if a covered entity intends to fundraise (with or without an authorization), it must include such a statement in its Notice of Privacy Practices
- CE's Notice of Privacy Practice must disclose that the organization may use PHI to contact the individual for fundraising and advise the individual that he or she has the right to opt out of receiving such communications.
 - Each communication must include a clear and conspicuous opportunity to elect not to receive any further communications.
- Opting Out
 - Fundraising communications sent out without an authorization must include a description of how the individual may opt out of receiving further communications
 - CE may not send fundraising communications to any individual who elects to opt out.
 - Opt out method must not cause individual to bear undue burden or incur more than a nominal cost. Flexible and not prescriptive standard
 - CE may provide information as to how to opt back in
 - CE can adopt a single or multiple opt-out methods as long as they are reasonably accessible to all individuals wishing to opt out
 - Use of toll-free number, email address, pre-printed, pre-paid return postcard are acceptable
 - Requiring a written letter is considered an undue burden
 - Opt-out may be applied on a campaign-specific or all fundraising basis

Direct from the Federal Regulations

paragraph (b)(1) and the introductory text of paragraph (b)(1)(v)(A);

- b. Add new paragraph (b)(1)(vi);
- c. Revise the introductory text of paragraph (e)(1)(iii) and paragraph (e)(1)(vi);
- d. Revise paragraph (i)(2)(iii); and
- e. Revise paragraphs (k)(1)(ii), (k)(3), and (k)(5)(i)(E).

The revisions and additions read as follows:

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

(b) *Standard: Uses and disclosures for public health activities.* (1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

(v) (A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer;

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains and documents the agreement to the disclosure from either:

(1) A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

(2) The individual, if the individual is an adult or emancipated minor.

(1) (iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph

(e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section.

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(E) Law enforcement on the premises of the correctional institution; or

■ 52. In § 164.514, revise paragraphs (e)(4)(ii)(C)(4), (f), and (g) to read as follows:

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(4) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that

apply to the limited data set recipient with respect to such information; and

(f) *Fundraising communications.* (1) *Standard: Uses and disclosures for fundraising.* Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

- (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.

(2) *Implementation specifications: Fundraising requirements.* (1) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.

(ii) With each fundraising communication made to an individual under this paragraph, 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 under this paragraph 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.

(g) *Standard: uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation,



2013 Changes to Fund Raising Components of HIPAA

By Joel L. Simon, January 21, 2013

On January 25, 2013, The Office of Civil Rights of The United States Department of Health and Human Service (“HHS”) will formally publish amendments to the regulations promulgated under The Health Insurance and Portability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2003 (HITECH). The essence of the regulations is that certain information may not be used nor disclosed by a health care provider (including hospitals and related foundations¹) except as allowed under HHS rules. Among the many areas impacted by these rules (billing, marketing, research, IT security, etc.) is fund raising. The amendments do not change the basic premise regarding protected information and fund raising, but they significantly modify the methods and practices that hospitals can or must employ when using regulated information for fund raising.

Basic HIPAA Rules Related to Fund Raising

HIPAA has governed fund raising since April 2003. As a general proposition, HIPAA protects “health information”. Health information is broadly defined as “any information, whether oral or recorded in any form or medium that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.” For purposes of this document, health information protected by HIPAA will be referred to as “PHI” (protected health information).

HIPAA rules allow hospitals to use PHI for “health care operations.” Fund raising is a part of health care operations. However to use PHI for fund raising, hospitals must comply with certain basic requirements, some of which are materially changed by the 2013 amendments. The basic requirements include: (1) that hospitals must provide a notice that it may use PHI to contact the individual to raise funds; (2)

¹ For purposes of this memorandum, “hospital” will refer to hospitals and their institutionally related foundation. HIPAA rules on hospital and foundation relationships were not changed materially by the 2013 Amendments.

that hospitals maintain a process to exclude persons who do not wish to receive fund raising communication from receiving such communication (known as “opt-out”); and (3) that only specific parts of PHI may be used for funds raising. Hospitals that violate HIPAA are subject to civil monetary penalties.

Amendments Overview and Dates

In 2010, HHS suggested multiple changes to parts of HIPAA that govern fund raising. Some of the suggestions, such as a requirement that patients have to “opt-in” to receive fund raising communication, are not part of the amendments that will be enacted. The fund raising related protocols that the amendments do change are (1) the method for individuals to opt-out of receiving fund raising communication; (2) the method of communicating a person’s right to opt-out from future fund raising communication; (3) how the hospital applies an opt-out election by an individual; (5) the type of PHI that a hospital may use for fund raising; (6) the contents of the hospital’s Notice of Privacy Practices; and (7) an express requirement that a hospital may not condition treatment on an individual’s choice to receiving fund raising communications.

These amendments are effective on March 26, 2013 with a compliance date of September 23, 2013. That means hospitals **may** use the modified practices allowed (or required) by the amendments on March 26. All of the amendments’ requirements **must** be complied with by September 23, 2013.

Opt-out Methods and Implementation

Current HIPAA rules require hospitals to include in all fund raising material instructions about how individuals may to opt-out of receiving future fund raising communications. The amendments are intended to strengthen the “opt-out” by requiring that the option be “clear and conspicuous” and that the opt-out method not cause an individual to incur an “undue burden or more than a nominal cost.” HHS intentionally did not specify the type of opt-out protocol a hospital must implement. This part of the amendment is intended to be flexible, not prescriptive. HHS has suggested that a toll-free (or local) call, an e-mail address, or a pre-printed pre-paid post card would be sufficient. Hospitals are free to choose the method that is best for them and their patients based upon size, geographic distribution, etc. of patient prospects. The new rule also allows a hospital to choose one method or multiple methods for patients to opt-out. Under the amendments, hospitals may no longer require that the opt-out be sent in writing by mail (as the current law specifies). While a written opt-out may not be required, it must be implemented if received.

Effect on current practices: (1) Hospitals must design and implement a new opt-out communication method or methods. A requirement that individual write to hospital is not allowed. Acceptable methods include (not exclusively): e-mail, toll-free or local call, or pre-printed and pre-paid postcard/mailed. Opt-out protocol must be

“clear and conspicuous” in all fund raising material. (2) Existing stock with current opt-out language must be used or destroyed by September 23, 2013. (3) Business Associate Agreements with direct mail vendors should be reviewed to ensure no terms need to be modified for compliance with new rules

As the method for receiving opt-out communication is flexible, hospitals have discretion in applying the scope of the opt-out election. Hospitals may restrict the opt-out to the specific campaign of the original communication, apply it to all future fund raising communications, or use some other policy. Hospitals may also provide individuals with the choice of opting out of all future fund raising communications or just campaign specific communications. Whatever method is employed, the communication should clearly and conspicuously inform individuals of their options (if any) and any consequences of electing to opt-out of fund raising communications.

Effect on current practices: (1) Hospitals should review fund raising strategy to design and implement an opt-out policy that is best suited to the organization and its strategy; (2) Hospitals should ensure the selected strategy is clearly and conspicuously included in the opt-out language used in fund raising communication.

The Amendments broadens the types of fund raising communications subject to opt-out notification. Previously, only written fundraising materials required opt-out instructions. Under the amendments **all** forms of fund raising communications must contain opt-out instructions. This includes telephone calls, other oral communication, and electronic communication, such as e-mail and social media communication that use lists created from PHI.

Effect on current practices: (1) Telephone solicitation scripts and e-mail or social media communications must be modified to include “clear and conspicuous” opt-out language; (2) Hospital staff calling for major gift cultivation appointment must include “clear and conspicuous” opt-out language; (3) Business Associate Agreements with telephone solicitation vendors and capital campaign counsel should be reviewed to ensure no terms need to be modified for compliance. Note that the use of opt-out language only applies to communications resulting from the use of PHI. Calls and e-mails to lists generated from outside the hospital (that is without PHI) are not governed by HIPAA.

Hospitals must comply with all opt-out requests. Under current rules, hospitals were only required to make “reasonable efforts” to comply with opt-out requests. Now, hospitals **must** implement the opt-out election. Reasonable efforts are no longer sufficient.

Effect on current practices: No material change of practice. The rule simply makes it a technical violation of the law not to comply with an opt-out election, regardless of the hospital’s “reasonable efforts.” (1) Business Associate Agreements

with vendors should be reviewed to ensure no terms need to be modified for strict compliance with opt-out elections.

Hospitals may (but need not) have a protocol (or a series of protocols) for people who have elected to opt-out to opt back in to future fund raising communication. Like the opt-out methods, hospitals have some discretion about how to communicate and implement opt-in elections. However, HHS has expressly stated the receipt of a new gift may not, alone, constitute an opt-in election nor may a hospital put an expiration date on opt-out elections as a method of having individuals opt back in to receiving fund raising communications.

Effect on current practices: (1) Hospitals should review its fund raising strategy to design and implement opt-in policy that is best suited to the organization and its strategy or determine that no opt-in protocol is desired.

Information that Can be Used for Fund Raising

The amendments include multiple changes in the type of PHI that may be used for fund raising. Most modestly, the amendments express what constitutes “demographic” information. Current rules allow the use of demographic information, but the rules themselves did not identify what constituted demographic information (they were part of a preamble). The amendments expressly specify the list of demographic information (name, address, other contact information, age, and gender) that are used in current practice.

The amendments also clarify that “date of birth” is demographic information and may be used for fund raising. Current law uses the term “age”, which caused confusion for some hospital compliance offices that did not want birth dates used in fund raising, just the static age.

Effect on current practices: None. These changes simply express provisions in the rules that existed by implication from the 2003 preamble. Note: if your hospital compliance office would not let you use the birth date of patient, just “age” you can now start sending birthday cards to donors and prospects.

The most significant change to the types of information that HIPAA now allows hospital fund raisers to use are the department of service used, the name of the treating physician, and (under limited circumstances) the outcome. HHS expressly did not define “department of service”, but intends the information to be limited to general department such as cardiology, oncology, or pediatrics that do not indicate a more specific diagnosis. Outcome information may only be used to screen and exclude from fund raising those patients who are deceased or had sub-optimal experiences. HIPAA broadly mandates that only the “minimum necessary information” be disclosed or used for any purpose. HHS reiterated that the non-

demographic PHI used and disclosed by the hospital to fund raise must meet this pervasive standard.

With the expanse of PHI that can be used in fundraising, databases may include a blend of both PHI and unregulated information. For example, if an existing donor becomes a heart patient, the name and address to solicit the donor (from a gift file) is not PHI, but the inclusion of the donor (as a patient) in a Heart Center solicitation is PHI. To comply with opt-out rules, hospitals need to be aware of the data source used to fund raise.

Effect on current practices: (1) Hospitals may cultivate major gift prospects based upon the department or physician they used; (2) Hospitals may create direct mail or phone solicitation lists based upon department of service or physician names; (3) Hospitals may create specific fund raising material and campaigns for certain former patients based upon the department and/or physician they used; (4) Protocols should be established with appropriate departments in the hospital to get lists of patients who died or had poor clinical or customer service outcomes – such list may only be used to purge fund raising lists; (5) donor database practices should be reviewed to determine how to distinguish between PHI and non-regulated data. (6) Business Associate Agreements must be reviewed to govern use of blended (PHI and unregulated) donor information.

Notice of Privacy Practice

Under existing HIPAA rules, hospitals must provide all patients with a Notice of Privacy Practices that contains numerous provisions about the use and disclosure of PHI, including that the hospital may use information to fund raise. Under the amendments, the Notice of Privacy Practice must also state that patient has a right to opt-out of receiving fund raising communication. The Notice does not need to specify the mechanism for opt out elections, merely that such right exists. Of course, the hospital is free to include methods for an opt-out election in the Notice.

Effect on current practices: (1) Coordinate with compliance office or department responsible for producing Notice of Privacy Practices to update the fund raising provision of the Notice to include: “[Hospital] may contact you to raise funds for [hospital]. You have a right to opt-out of receiving such communications.” Note that this language is suggested not mandated and the hospital may include method to opt-out in the Notice. (2) Ensure that current Notice of Privacy Practices are used or destroyed by September 23, 2013.

Conditioned Fund raising

The amendments express an implied rule: that a hospital may not condition treatment or payment on an individual’s choice with respect to receiving fund raising

communications. That is, hospitals may not treat those who elect to opt-out differently than those who do not.

Effect on current practices: None. This change simply expresses a provision in the rules that existed by implication.

Selected Provisions of HIPAA Fund Raising Rules as Amended

45 C.F.R § 164.514(f) Fundraising Communications

(1) *Standard: Uses and disclosures for fundraising.* Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

- (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.

(2) *Implementation specifications: Fundraising requirements.*

(i) A covered entity may not use or disclose protected health information for fund raising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.

(ii) With each fund raising communication made to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fund raising communications. The method for an individual to elect not to receive further fund raising 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 fund raising communications.

(iv) A covered entity may not make fund raising communications to an individual under this paragraph 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 fund raising communications with a method to opt back in to receive such communications.

45 C.F.R. § 164.520 Notice of privacy practices for protected health information

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt-out of receiving such communications.