

Fundraising Under HIPAA

**Practical guidelines for U.S. health care development professionals
on how to achieve fundraising success while staying in compliance
with the Health Insurance Portability and Accountability Act.**

Updated according to modifications to the HIPAA Privacy, Security,
Enforcement, and Breach Notification Rule released January 25,
2013 and effective on March 26, 2013.





Fundraising Under HIPAA

AHP RESEARCH TO PRACTICE GUIDE

While the publisher and author have used their best efforts in preparing this guide, they make no representations or warranties with respect to the accuracy or completeness of the contents of this publication. Neither the publisher nor author is engaged in providing legal or other professional services. The services of a qualified legal professional should be sought for legal advice.

The Association for Healthcare Philanthropy is the leading authority for standards, knowledge and leadership in health care development. AHP's 5,000 members represent more than 2,200 health care facilities in the United States and Canada. They embody all aspects of health care fundraising, from executive directors and chief development officers, to major gift officers, annual campaign managers, event coordinators and grant writers.

For more information about AHP, visit www.ahp.org or call (703) 532-6243.

Editorial director: Catherine E. Gahres, MBA (first edition);
Cindy Moon-Barna, MLSIS and Kathy Renzetti, CAE (second edition)

Book design: Accordant Philanthropy

Association for Healthcare Philanthropy
313 Park Avenue, Suite 400
Falls Church, VA 22046
(703) 532-6243
www.ahp.org

© 2013 The Association for Healthcare Philanthropy (second edition)
ISBN 978-0-9853211-4-7

© 2012 The Association for Healthcare Philanthropy (first edition)
ISBN 978-0-9853211-2-3

Printed September 2012 (first edition), March 2013 (second edition)

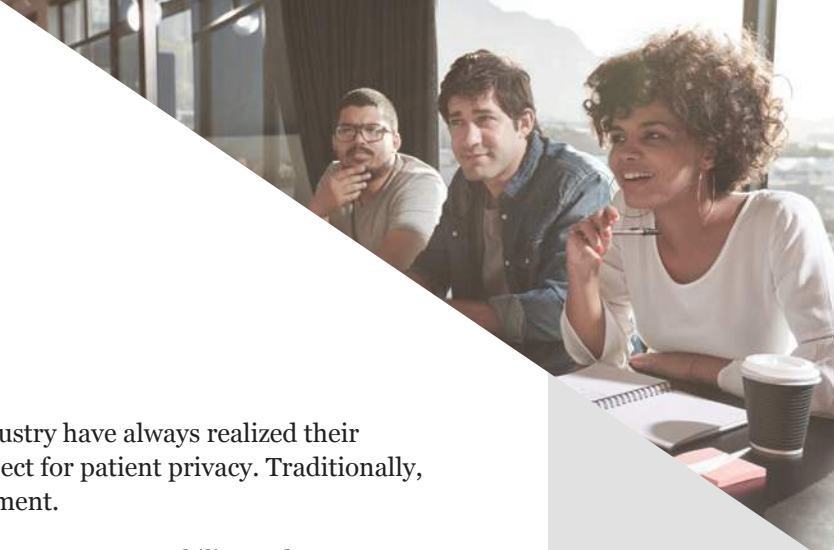
All rights reserved. No portion of this publication may be reproduced or used in any form, electronic or mechanical, including photocopying or recording, without written permission from the Association for Healthcare Philanthropy (AHP). Permission may be obtained by writing to AHP at 313 Park Ave., Ste 400, Falls Church, VA 22046, or by email to ahp@ahp.org.

Table of Contents

Foreword	5
About this Guide	6
HIPAA: The Basics	7
HIPAA's purpose and intent	7
The role of HHS and the regulatory history	7
Who is subject to the HIPAA 2002 Privacy Rule?	8
HIPAA's impact on fundraising	8
Important terms	9
Fundraising and Protected Health Information (PHI)	11
The minimum necessary standard	11
Patient information that can be used for fundraising without patient authorization	12
Use of PHI for fundraising that requires patient authorization	13
Patient authorization form	14
State and other federal privacy laws	14
Filtering PHI data—what's permissible	14
Use of data “matching” services	15
Use of patient directory and daily census report	16
“Rounding” and incidental disclosure	16
Physician, nurse and technician referrals	17
Physician involvement in fundraising	17
Donor “shadow” programs	19
Use of PHI in applying for grants	20
Soliciting long-term care patients' family members	20
Soliciting a health care provider's employees or a teaching hospital's alumni	20
When in doubt...	20
Notice of Privacy Practices	21
Required contents of a Notice	21
Sample language	22
Availability of the Notice	22
Patient acknowledgement of receiving the Notice	22

Table of Contents CONTINUED

Opt-out Provision	23
Requirements	23
Sample language	24
Languages other than English	24
Scope of the opt-out	25
Expiration of the opt-out	25
Non-written patient opt-out requests	25
Honoring patient opt-out requests	25
Opt-out provisions and invitations to special events	26
Inviting opted-out patients to educational events	26
Newsletters, brochures and general audience communications	26
Planned giving communications	26
Opt-out requirement once a patient becomes a donor	27
Penalties for not honoring opt-out requests	27
Opt-in requirement	27
Fundraising Vendor and Business Associate Agreements	28
Important terms	28
Distinction between an institutionally related foundation and a business associate	29
Fundraising vendors and business associate agreements	30
Volunteers and business associate agreements	31
HIPAA business associate agreement specifics	31
Business associate and subcontractor liability	31
Marketing and the Privacy Rule	32
Definition of marketing	32
Distinction between marketing and other activities	33
Avoiding risk in marketing	33
Breaches, Notification and Penalties	34
Definition of a breach	34
Required risk assessment	35
Notification of breach requirements	36
Penalties	37
Appendix A—Definitions	38
Appendix B—Sample Patient Authorization Form	44
Appendix C—Sample HIPAA Business Associate Agreement	46
Appendix D—Clarifying Letter from HHS to AHP	53
HIPAA Checklist	Inside Back Cover

A photograph of three people—two men and one woman—sitting around a table in a meeting. The woman on the right is smiling and gesturing with her hand. The man in the middle is looking at her, and the man on the left is looking towards the camera. There are notebooks and a coffee cup on the table.

Foreword

Fundraising professionals in the health care industry have always realized their responsibility to balance their efforts with respect for patient privacy. Traditionally, striking the right balance was a matter of judgment.

That changed with the enactment of the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA). The legislation laid the groundwork for establishing specific regulations—which were finalized in 2002 with the Privacy Rule and substantially modified in 2013—for protecting patient medical information and setting civil and criminal penalties for violations.

This guide is designed to help health care development professionals understand, apply and comply with HIPAA regulations and standards. Its broad objective is to provide education that will aid in compliance and to demonstrate that the Association for Healthcare Philanthropy (AHP) and the health care development profession is committed to respecting patient privacy while raising support for the health care resources of America's communities.

If your organization is firmly established and operating a successful grateful patient program, this guide will help you determine if you are in compliance with current HIPAA regulations. If you are just starting your patient outreach efforts, this guide will give you a solid foundation for building your program. It offers the basic information you need in support of your grateful patient program as you work with your staff, board and volunteers, and the technology officers, privacy officers and attorneys in the health care organization you support.

As with all legislation, HIPAA has evolved over the past decade and will continue to do so. As the regulations governing fundraising and patient privacy change, so will this publication. This edition includes the modifications published as a final rule on January 25, 2013, effective on March 26, 2013.

Our thanks to AHP legal counsel, Peter Parvis, J.D. of Venable, LLP for his review of the first and second editions of this publication; to the AHP members that served on the editorial review group for the first edition of this publication (Joel L. Simon, J.D.; Pamela J. Pratt, CFRE; Mark D. Belcher; Marite Butners, J.D. LLM; Arline M. Stephan; and B. J. Leber); and our writers and editors, Catherine Gahres, MBA (first edition), Cindy Moon-Barna, MLSIS and Kathy Renzetti, CAE (second edition). Special thanks to AHP president emeritus, William C. McGinly, Ph.D., CAE, who oversaw this guide's original development and production.

Steven W. Churchill, MNA
President and Chief Executive Officer
Association for Healthcare Philanthropy

About this Guide

The information in this guide is for educational purposes and is intended to provide general information and guidance. This guide is not intended to provide legal advice.

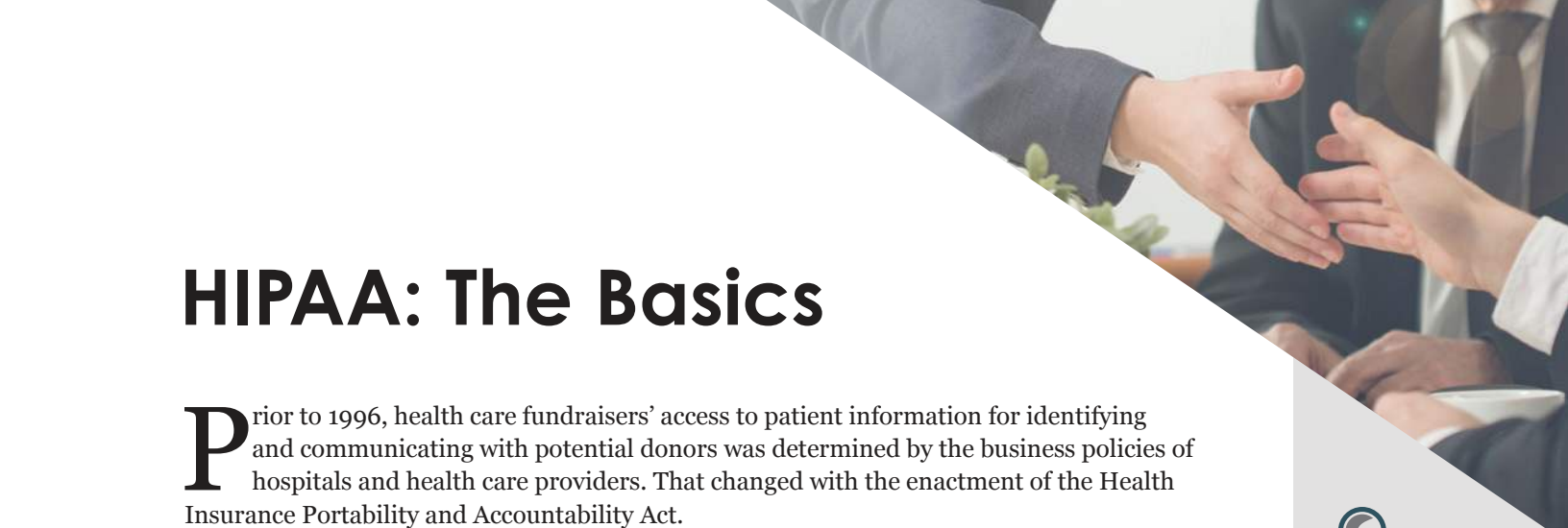
HIPAA, as with all regulations, was written to provide clarification and guidance, but it does not identify and clarify all situations and circumstances. Interpretations vary and organizations should make decisions regarding their business practices and HIPAA compliance based on their unique circumstances.

The guide is based on review of the U.S. Health Insurance Portability and Accountability Act (HIPAA) 2002 Privacy Rule; the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act; HIPAA regulation changes released by the Department of Health and Human Services Office of Civil Rights (HHS/OCR) as of March 1, 2012, 2013 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rule (the "Modified Rule"); and clarifying information that HHS has provided in response to AHP inquiries. *This guide is written assuming a conservative reading of HIPAA regulations and a low organizational tolerance for risk.*

HIPAA is just one of many laws that address patient privacy. This guide does not discuss state laws or other federal laws that may have an impact on individual situations. State privacy and confidentiality statutes limit the release of patient records in most states and other federal laws place explicit limits on certain types of medical information, most notably in the areas of HIV, substance abuse, behavioral medicine and abortion.

If you have questions about or suggestions for this guide, please direct them to:

Association for Healthcare Philanthropy
313 Park Ave., Suite 400
Falls Church, VA 22046
703-532-6243
ahp@ahp.org



HIPAA: The Basics

Prior to 1996, health care fundraisers' access to patient information for identifying and communicating with potential donors was determined by the business policies of hospitals and health care providers. That changed with the enactment of the Health Insurance Portability and Accountability Act.

HIPAA's purpose and intent

Recognizing the need for national patient privacy standards, the U.S. Congress provided for such protections in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Among other things, HIPAA regulations establish specific requirements for protecting patient medical information and set civil and criminal penalties for violations. The fundamental intent of the Privacy Rule is to ensure that health care providers and insurers use extreme care in protecting the confidentiality of patient information and use only the minimum necessary patient information required to accomplish operational tasks.

The role of HHS and the regulatory history

HIPAA designates the U.S. Department of Health and Human Services (HHS) as the authority for developing rules and standards to enforce HIPAA and for interpreting the legislation for the benefit of both patients and health care providers.

HHS proposed HIPAA-compliant federal privacy standards in 1999, and, after considering more than 52,000 comments, published the Privacy Rule in December 2000. HHS released modifications to the Privacy Rule in August 2002. HHS subsequently issued the Security Rule in February 2003, and the Enforcement Rule in April 2003, which was later amended in February 2006 and again in October 2009.

The Health Information Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act of 2009 (ARRA), made a number of changes to the HIPAA Privacy, Security and Enforcement Rules and HHS was required to issue regulatory guidance related to these changes. New regulations regarding breach notification were finalized in 2009, and HHS announced additional proposed rules in July 2010, which included changes to the fundraising section of the Privacy Rule. Those proposed changes were finalized on January 25, 2013 with the release of the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, effective on March 26, 2013. The changes are substantial and largely beneficial, and this edition of the guide incorporates the changes.



More information on HIPAA can be found on the HHS website at <http://www.hhs.gov/hipaa/>.



Who's responsible?

A hospital or health care provider is defined as a "covered entity" under HIPAA and therefore subject to and responsible for HIPAA regulations as they pertain to fundraising—whether fundraising resides as an internal department or is handled by an institutionally related foundation.



The HIPAA Privacy Rule regulations include fundraising "for benefit of the covered entity" as a "health care operation," [45 CFR § 164.501] and describe the types of information that may be used or disclosed in connection with fundraising activities. [45 CFR § 164.514(f)].

Who is subject to the HIPAA Privacy Rule?

HIPAA uses the term "covered entities" to describe those organizations which are subject to HIPAA and the Privacy Rule. A covered entity is any one of the following types:

- **Health care provider**—individuals or organizations that furnish, bill or are paid for furnishing health care services in the normal course of business, such as hospitals, clinics, doctors, dentists, nursing homes and home health care providers, and that *transmit health information in electronic form*, either directly or through a third party, for claims, billing, benefit eligibility inquiries, referral authorization requests, and other transmissions outlined in the HIPAA Transactions Rule.
- **Health care clearinghouse**—public or private entities, including billing services, community health management and health information systems, that receive or process health information.
- **Health plan**—an individual or group plan that provides or pays for the cost of medical care, including HMOs, health insurance companies, company health plans, and government programs that pay for health care, such as Medicare, Medicaid and military and veteran health care programs.

HIPAA's impact on fundraising

HIPAA *did not* take away the ability for a hospital or health care organization, or its institutionally related foundation, to contact patients for fundraising purposes. However, it defines the type of patient information that can be used or disclosed and provides for greater patient awareness and control of their information.

Under the Modified Rule:

- A health care provider or its institutionally related foundation may use or disclose for its own fundraising purposes *demographic patient information, health insurance status, the patient's dates of service, department of service information, treating physician information and outcome information* without patient authorization. 
- Prior to using allowed patient information for fundraising purposes, a hospital or health care organization must provide that patient with a copy of the health care provider's Notice of Privacy Practices, *which includes the statement that they may be contacted for fundraising efforts* and that they may elect not to receive fundraising materials ("opt out"). The specifics of the opt-out may, but are not required to, be included in the Notice of Privacy Practices.
- Each fundraising communication that a health care provider or its institutionally related foundation makes (including any oral or telephonic communication) to patients must include an opt-out provision that describes how the patient can discontinue receiving fundraising materials and solicitations from the health care provider or its related foundation. Although the provider can select the opt-out (or opt back in) method, it cannot impose a burden on the recipient. *(See discussion of this point in the Opt-out Provision section on page 23)*

Important terms

Protected Health Information (PHI)

PHI is defined as patient information that meets the following criteria:

- › Electronically transmitted or stored information;
- › Created or received by a health care provider—written or oral;
- › Related to the past, present or future physical or mental condition of an individual, or the provision of health care for an individual; and that
- › Includes demographic information, which can be used to identify the individual.

PHI includes demographic information, dates of service, diagnosis, nature of services, medical treatment department and other information that may reveal the identity of the individual or any facts about his or her health care or health insurance. HIPAA allows only demographic patient information, health insurance status, dates of service, department of service information, treating physician information and (for limited purposes) outcome information to be used for fundraising purposes without written patient authorization.

NOTE: Information obtained by a development department or related foundation not related to a patient's treatment or stay, their physical condition or health care, such as an address on a donor check, is not covered by HIPAA. For example, if the development department in its fundraising materials sent to patients invites individuals to self-identify areas of interest, the information freely provided by the patient may be used for fundraising purposes. Moreover, materials sent using mailing lists that do not come from the covered entity nor include any health care information that could identify the individual are not subject to the HIPAA rules.

NOTE: The Privacy and Security Rules do not protect individually identifiable health information of persons who have been deceased for more than 50 years.

Demographic information

Demographic information includes a patient's name, address, other contact information such as phone numbers and email address, age, gender, and date of birth. HIPAA permits such non-medical identifying information to be used for fundraising efforts without patient authorization. The rule also allows the use of a patient's insurance status, although in the rule it does not constitute demographic information.

NOTE: Patient demographic information is protected health information and should be treated in accordance with HIPAA regulations for safeguarding its use and disclosure beyond what is essential for the operation of fundraising activities. If a business associate is used to assist in fundraising, (1) the hospital must have a business associate agreement with that entity (even if it contracts directly with the related foundation), (2) have "satisfactory assurances" that the business associate and foundation are complying with HIPAA regulations, and (3) can only disclose to those entities the minimum necessary information to accomplish their tasks.



Opt-out:

HIPAA regulations state that "a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications " "with each fundraising communication made to an individual under this paragraph." [45 CFR § 164.514(f)(2)]

Notice of Privacy Practices (Notice)

HIPAA requires health care providers to develop and make available to patients a Notice of Privacy Practices that provides a clear explanation of the health care provider's privacy practices and the patient's rights regarding their protected health information. This Notice must include information about fundraising practices if a hospital, health care organization or its institutionally related foundation intends to send fundraising communications to patients. The Notice also must state that a patient will have the right to opt out of receiving such communications.

Opt-out provision

HIPAA requires a health care provider or its institutionally related foundation to include in *each* fundraising communication (written or oral) it provides patients, language that describes how the patient may stop receiving any further fundraising communications (the opt-out). The opt-out mechanism cannot impose a burden on the recipient. The Modified Rule in the preamble states that requiring the recipient to mail a letter to opt out **is an undue burden**. A local phone number, toll-free number, e-mail address, pre-printed, pre-paid postcard or similar approach that is "simple, quick and inexpensive," or any combination of such approaches can be used. However, the health care provider or its institutionally related foundation must have a system in place to track and apply all opt outs, since making a fundraising communication to a recipient who has opted out is a violation of HIPAA. The health care provider or institutionally related foundation may elect to have an opt out for a specific campaign or for everything, but once again it is expected to have a system in place to ensure compliance. The preamble advises that a hospital or other covered entity may wish to consider its demographics, including English proficiency, to determine both its Notice and the opt-out mechanisms it adopts. 

Opt-in provision

The Modified Rule permits, but does not require, a covered entity to have an opt back in policy. The preamble suggests that an entity could put a call in number on a routine newsletter sent to all patients (which did not contain a fundraising solicitation) that patients could call to be put on (or back on) a fundraising list.

Fundraising and Protected Health Information (PHI)

Prior to HIPAA, a health care provider's development office or institutionally related foundation and fundraising business associates often had access to patient health information for the purpose of identifying and targeting prospective donors. The HIPAA Privacy Act limited this access by establishing strict standards and regulations regarding the disclosure and use of patients' protected health information (PHI).

This section discusses

- › The minimum necessary standard
- › PHI that can be used without patient authorization
- › PHI that requires patient authorization prior to use
- › Patient authorization form
- › State and other federal privacy laws
- › Filtering of PHI for fundraising purposes
- › Use of data matching services
- › Use of patient directory and daily census report
- › Rounding and incidental disclosure
- › Physician, nurse and technician referrals
- › Physician involvement in fundraising
- › Donor shadow programs
- › Use of PHI in applying for grants
- › Soliciting family members of long-term patients
- › Soliciting health care employees and teaching hospital alumni

The minimum necessary standard

One of the guiding principles behind the HIPAA Privacy Rule is the “minimum necessary standard.” This standard requires a health care provider to limit the use, disclosure of and requests for *protected health information* to the minimum necessary to accomplish legitimate tasks.

The Privacy Rule generally does not try to define the minimum standards. Rather, it leaves flexibility for covered entities to develop and implement policies and procedures needed to limit unnecessary or inappropriate access to, and disclosure and use of protected health information, based on each entity's unique operational model and workforce.



The 2013 Modified Rule states that 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... (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; (v) Treating physician; (vi) Outcome information; and (vi) Health insurance status. [45 CFR § 164.514(f)]

However, in the case of fundraising, the HIPAA Privacy Rule *does* help clarify the minimum standard by imposing restrictions on the use of PHI, and allowing only the use of patient demographic information, health insurance status, dates of service, department of service information, treating physician information and outcome information.

Regulators have provided clear guidelines based on the Modifications released in January 2013 that patient demographic information, health insurance status, dates of service, department of service information, treating physician information and outcome information CAN be used for fundraising purposes based on an appropriate Notice of Privacy Practices, but that other patient *medically related* information CANNOT be used for fundraising efforts unless the health care provider obtains patient authorization. However, for fundraising practices that are not so clear-cut and require interpretation, applying the minimum necessary standard is a good start to staying in compliance and minimizing risk.

Patient Information that can be used for fundraising without patient authorization

Six categories of patient health information may be disclosed or used for fundraising purposes without a patient's written authorization:

- Patient demographic data
- Health insurance status
- Dates of patient health care services
- General department of service information
- Treating physician information
- Outcome information

Patient demographic data includes:

- Name
- Address
- Other contact information (phone numbers, email address, etc.)
- Date of birth
- Age
- Gender

HIPAA regulations do not provide clarification or guidance regarding the definition of "insurance status." AHP's legal counsel has interpreted "insurance status" to include not only whether a patient is insured but also the type of insurance.

As with all other patient information, the minimum necessary standard always applies. Therefore, insurance status should be requested by or given to a development office, related foundation or business associate only if it is reasonably necessary to perform a specific fundraising task. As an example, knowing that an individual is a Medicaid patient likely would be essential to fundraising efforts to avoid inappropriate contact.

NOTE: Even though patient authorization is not required when using the categories of information discussed above, a health care provider or its related foundation *may not send fundraising materials to a patient until the health care provider has provided that patient with a copy of their Notice of Privacy Practices*. The Notice must include language that patient information may be used for fundraising purposes and that the patient will have the right to opt out from receiving fundraising communications. The health care provider must make a reasonable effort to obtain the patient's acknowledgement of receiving the Notice (see page 21 for more information on the Notice). The Notice is sufficient to send the initial fundraising communication to the patient, although that first communication (and each subsequent communication) must contain the opt-out provision. There is no requirement that the recipient opt in before making the first communication.

The Modifications to the Privacy Rule released in January 2013 allow for covered entities to use department of service information, treating physician information and outcome information for fundraising purposes in order for fundraisers to target their communications to appropriate individuals. The Modified Rule clarifies that department of service information includes information about general department of treatment, such as cardiology, oncology or pediatrics. The Preamble clarifies that the intent of including outcome information in the PHI that can be used or disclosed is to permit covered entities to use (or disclose to related foundations or business associates) outcome information such as death or other sub-optimal result **ONLY** to screen and eliminate patients or families from receiving fundraising materials.

Use of PHI for fundraising that requires patient authorization

A patient's written authorization is required before a fundraising entity can use protected, medically related health information to filter, target, use or disclose as part of fundraising efforts. PHI that requires patient authorization prior to use for fundraising includes, but is not limited to:

- Diagnosis
- Nature of services
- Treatment

Examples of fundraising efforts that *require patient authorization*:

- A personalized appeal letter to a patient, which mentions a specific disease, condition or treatment related to the patient. For example, language such as, "As a breast cancer survivor, you know the importance of..." We note, however, that oncology is one of the departments referenced in the Preamble, so the department of service could be used to filter cancer survivors, albeit without a reference to their condition or treatment.
- For example, we note that filtering or targeting by department is acceptable. A fundraising letter for a new cancer center sent to a list of former oncology patients treated in the oncology department would be acceptable because it used the department of service.



No "opt-in" required:

Authorization for use of patient medically related information is sometimes referred to as an "opt-in." It's important to note that an "opt-in" is NOT required under HIPAA for use of demographic patient information, health insurance status, the patient's dates of service, department of service information, treating physician information and outcome information for fundraising efforts although a hospital may "provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications."

Patient authorization form

A development office or supporting foundation can use patient diagnosis, nature of services, or treatment in fundraising efforts as long as *written patient authorization has been obtained by the health care provider*.

The authorization form should include the names of all organizations that will be using the information for fundraising efforts, how the information will be used, specifically what medical information will be used (full record, department or diagnosis data, etc.), as well as other standard HIPAA requirements for a medical records release authorization. A sample authorization form is provided in Appendix B. Authorizations are freely revocable, although a revocation does not have any impact on the actions taken in reliance on the authorization prior to its revocation.

NOTE: HITECH specifies that treatment or coverage can never be conditioned based on authorization. The hospital or health care provider cannot make decisions about patient treatment or coverage based on the patient's decision to authorize, or not authorize, use of their medically related information for fundraising. The Modifications to the Privacy Rule (January 2013) similarly prohibit the conditioning of treatment or payment on an individual's choice with the respect to the receipt of fundraising communications.

State and other federal privacy laws

Health care providers and supporting foundations should keep in mind that the HIPAA Privacy Rule does not preempt state laws, or other federal laws, that may be more restrictive.

For example, HIPAA permits limited disclosure of hospital patient directory information, but other federal laws (for example, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970; the Drug Abuse Office and Treatment Act of 1972; 42 Code of Federal Regulations Part 2, 188) prohibit a health care provider from releasing any information regarding a patient being treated for alcohol or substance abuse.

Filtering PHI data—what's permissible

HIPAA allows hospitals, health care organizations and their supporting foundations to use, *without a patient's authorization*, patient demographic information, health insurance status, dates of service, department of service information, treating physician information and outcome information. Therefore, unless a health care provider has secured additional authorization, it may only filter patient data for fundraising purposes using the criteria discussed above.

For example, the following filters are permissible without additional patient authorization:

- › By address data to target patients in a specific geographic region or zip code.
- › By address data to avoid contacting individuals at specific addresses, such as nursing homes or substance abuse treatment facilities.
- › By age to avoid soliciting donations from minor patients, or to target patients in a specific age range.
- › By insurance status to avoid soliciting donations from Medicaid patients.
- › By department of service, but not by diagnosis or treatment.
- › By treating physician.

It is important that the permissible filtering is not done in concert with other efforts that generate lists based on patients' illnesses, treatments or services received, unless additional written patient authorization has been obtained.

Filtering to avoid inappropriate fundraising

Prior to HIPAA, it was considered acceptable and even a best practice to omit from fundraising efforts patients treated in psychiatric or in alcohol or drug rehabilitation departments because such contact was considered inappropriate. However, the HIPAA Privacy Rule originally did not allow for filtering by department or medically related information without prior patient authorization. The Modified Rule permits use of departmental status to filter information, so data can be filtered on the basis either of treating physician or department of service to avoid inappropriate fundraising solicitations. HIPAA does not supersede more restrictive provisions of law, so laws pertaining to the protection of alcohol or drug rehabilitation units or certain sexually transmitted diseases will still apply.

Use of data “matching” services

HIPAA allows health care organizations and their related foundations to use patient demographic information, health insurance status, dates of service, department of service information, treating physician information and outcome information for fundraising operations (“permitted patient information”), which includes normal fundraising activities such as the use of third-party vendors for direct mail or wealth screening services.

Using “look-up” or “matching” databases or services for address verification or wealth screening is allowed under HIPAA as long as only permitted patient information is disclosed or used in the process, and the fundraising organization and any third-party vendor involved are in HIPAA compliance regarding safeguarding the patient information. In addition, any fundraising vendor must have a business associate agreement with the health care provider, which outlines the vendor’s responsibilities under HIPAA. However, outcome information should generally not be shared with such entities, although a list of “do not mail” names could be provided without explanation to permit the foundation or business associate to perform their task. The Modified Rule changes the definition of business associate and imposes the requirement that hospitals obtain reasonable assurances from business associates and subcontractors of business associates (who are now considered business associates in their own right if PHI will be disclosed to them) that such entities will comply with HIPAA and require additional effort if the related foundation or business associates or subcontractors will have access to PHI.



Patient directory:

From a business perspective, patients who have informed the institution that they do not want any information about themselves disclosed in a directory may assume that their request applies to the development organization as well. A clear policy should be created regarding this situation and staff prepared to answer any questions from patients.

Use of patient directory and daily census report

Many development offices or related foundations use their hospital or health care organization facility patient directory or daily census data for fundraising purposes, including:

- Identifying donors or prospective donors for development office or foundation concierge or VIP programs.
- Identifying donors or prospective donors for visits or rounding by development personnel.

Patient demographic data and dates of service from a daily census report can be provided to the development office or related foundation for fundraising purposes in accordance with the HIPAA Privacy Rule.

Likewise, the development office or related foundation can have access to patient directory information. However, there are some varying legal interpretations of the regulations regarding the way patient directory data can be shared—as a compiled data listing or as individual patient inquiries—and if shared as a data listing, what data can be provided.

Use of patient directory information involves interpretation of two separate aspects of the HIPAA regulatory language: 1) HIPAA allows a hospital or health care organization to maintain a patient directory and share, with the patient's authorization, limited information about location and general health with anyone who inquires about a patient by name; and 2) HIPAA allows a hospital or health care organization to share and use for fundraising purposes patient demographic information and dates of service.

AHP legal counsel's interpretation is that the two aspects of the regulations when considered together allow for the sharing of patient directory information, including location, for fundraising purposes because the information is consistent with demographic information and the intent of HIPAA in relation to use of patient information for fundraising. Note however that the patient has the right to tell the covered entity NOT to include them on the directory, which would prohibit using or disclosing directory information (but not permitted patient information) about such patients. However, some health care organizations have focused more exclusively in their interpretations on the directory use regulations and limit fundraisers' access to facility patient directories to individual requests by patient name. You should clarify your health care organization's policy with your privacy officer.

“Rounding” and incidental disclosure

Development office or foundation personnel that visit donors or prospective donors in a hospital or health care facility must ensure that any medically related information that is inferred, accidentally overheard or viewed during a visit is kept confidential and *not used or disclosed* for fundraising purposes, unless the patient provides permission. Moreover, the Modified Rule requires in EVERY instance, oral or written, that the recipient be informed of their right to opt out of receiving fundraising information. Use of scripts for telephonic or oral solicitation must include a description of this right and the method(s) selected by the hospital or health care institution for the patient to elect to opt out.

Great care also should be taken with any medically related information that a patient or family member shares with fundraising personnel during a visit. While it presents less risk under HIPAA, since a patient is free to provide personal information and once shared it is no longer protected under HIPAA, patients may assume a level of confidentiality. From a business perspective, it is advised that fundraising personnel obtain a patient's permission before using or disclosing medically related information obtained during a visit for fundraising efforts.

Physician, nurse and technician referrals

A physician, nurse or technician is allowed to provide a patient's name, as well as other permitted patient demographic information, to the health care provider's development office or institutionally related foundation for fundraising purposes without patient authorization, *as long as*:

- The physician, nurse or technician is an employee of the hospital or health care organization or participates in an organized health care arrangement (OHCA) with the hospital or health care organization; and
- The patient has been treated at the hospital or health care organization;
- The hospital or health care organization's Notice of Privacy Practices indicates that patient information may be used for fundraising purposes.

HHS, in an April 2, 2003 letter to AHP in response to a request for clarification regarding physician referrals, noted that a physician who is not a member of the health care organization's workforce, but who participates in an OHCA, may share patient information for purposes of fundraising. The information shared, however, must be limited to demographic information and dates of service. The information that may be disclosed has been expanded under the Modified Rule, so any information that can be used by the hospital or health care institution could be conveyed by the treating physician, including the treating physician himself or herself. 

If a physician is not an employee of the hospital or health care provider, and does not participate in an OHCA relationship with the hospital or health care provider, then the physician should not share patient information for fundraising purposes with the health care providers' development office or supporting foundation without written patient authorization.

The physician as a covered entity cannot disclose patient PHI to assist *another* covered entity's fundraising efforts without patient authorization.

Physician involvement in fundraising

HIPAA permits physicians to provide patient names to the health care organization's development department or related foundation for fundraising purposes as long as they are employees or participate in an OHCA. However, questions arise regarding the extent to which a physician may share his or her patient information and the degree to which a physician can take an active part or the lead in fundraising for a health care organization.

This issue can be very complex, so you should review any fundraising efforts that involve physicians with your health care organization privacy officer. That said, below is guidance from AHP legal counsel based on its interpretation to get you started:



HHS clarification regarding physician referrals:

"...If the covered entity and the health care provider, who is not a member of the covered entity's workforce, participate in an organized health care arrangement (OHCA), the provider may disclose [demographic patient information, health insurance status, the patient's dates of service, department of service information, treating physician information and outcome information] health information for any health care operation activities of the OHCA." [See Appendix D for a copy of the clarification letter.]



Fundraising for another covered entity:

"A covered entity may use or disclose to a business associate or to an institutionally related foundation... [the specified protected health information] for the purpose of raising funds for its own benefit..." [45 CFR § 164.514(f)(1).] The preamble to the Privacy Rule provides further clarification with the example that a physician cannot use PHI to send fundraising materials for an unrelated charity that supports research, since that would be fundraising for another covered entity.

Physician sharing of patient list

While HHS did not specifically address this issue in its clarification to AHP in 2003 or in the Modified Rule, AHP legal counsel's interpretation is that an employed physician or a physician who is a member of an organized health care arrangement (OHCA) may share their patient list for fundraising purposes *assuming the following two conditions are met*:

1. The patients must have been treated at the health care organization or hospital and have received the appropriate Notice of Privacy Practices from the health care organization or a joint Notice from the OHCA. The physician may NOT share information regarding his or her patients who have NOT been treated at the hospital or health care organization without patient authorization.
2. The relationship between the patient and the physician must be treated as incidental disclosed information—any medically related information inferred from the physician name cannot be disclosed or used, except for targeting or filtering. The Modified Rule permits the use of treating physician for fundraising efforts, but not the services that the physician provided.

Physician involvement in fundraising appeals and activities

HIPAA imposes limits on physician involvement in fundraising efforts for a hospital or health care organization. These limitations are primarily dictated by the physician's legal relationship with the health care organization and if patient authorization has been obtained to fundraise on behalf of another entity. Unless patient authorization has been obtained, HIPAA only allows a covered entity (a hospital, health care organization or a physician) to fundraise for its own benefit. 

Below are several scenarios of physician involvement with direct mail campaigns with AHP legal counsel's interpretation regarding compliance under HIPAA:

Example #1: ABC Hospital foundation sends a letter to a *general hospital patient list* that is from a physician *employed by ABC Hospital*.

The above example is allowable under HIPAA assuming the development office or related foundation is in compliance with normal HIPAA requirements. From a HIPAA perspective, the physician's involvement is no different than sending a testimonial letter from any hospital employee to a general patient listing. Of course, other legal issues should be examined, including authorization to use the physician's name or signature and appropriately identifying the physician as an employee of the hospital. The letter must include an opt-out provision.

Example #2: A physician *employed by ABC Hospital* sends a fundraising letter to *his or her patients* in support of an ABC Hospital campaign OR the development department sends the letter on the physician's behalf.

The physician or development office can send such a letter only if the physician's patients receiving the letter have been treated at ABC Hospital by the physician.

The name of the treating physician is identified under HIPAA as a criterion for filtering or targeting for fundraising without written patient authorization. As always, any specific information about diagnosis or treatment by the physician cannot be used

without patient authorization. Outcome information can be used, but only to filter the recipients of the fundraising communication.

The letter must include an opt-out provision.

Example #3: A physician that is *not an employee* of ABC Hospital but is *part of an OCHA* with ABC Hospital sends a *personal fundraising letter* to *his or her patients* in support of an ABC Hospital campaign.

The physician can send such a letter only if all of the following conditions are met:

1. The physician has received authorization from his or her patients to use their information for fundraising purposes on behalf of ABC Hospital; OR has given the patients a Notice of Privacy Practices that includes compliant language regarding the fundraising activity; OR the patient has received notice as part of a joint OHCA Notice of Privacy Practices and the physician limits his mail list to individuals who are both patients of the physician and the hospital.
2. The physician's fundraising letter includes an opt-out provision and the physician is prepared to handle and track such requests. Since the letter is personally from the physician, and he is using his own patient list, the physician must make arrangements to track opt outs to ensure that he does not mail a fundraising appeal to these patients in the future.
3. The physician does not use or disclose any information about diagnosis, treatment or outcome. As before, a letter that states anything such as "as a former [insert disease] survivor" is not permitted without patient authorization.
4. The opt-out language is included.
5. The physician will not benefit from fundraising efforts paid for by the hospital or health care organization in a way that would pose a violation under federal Stark regulations.

In the above examples, where a physician sends a fundraising appeal, the responsibility to comply with HIPAA—and any associated risk—rests with the physician as a covered entity. However, a development office or related foundation shares the responsibility and risk if it has knowledge of, participates in or encourages such activity. Therefore, if your development organization knows of or is involved in physician fundraising efforts to support your health care organization, you must ensure that the physician is in compliance with HIPAA. Given the difficulty the physician would have in complying with opt outs, and the penalties that may be imposed for failure to comply with an opt out, it is our recommendation that all communications come from and in the name of the hospital or related foundation.

Donor “shadow” programs

Many hospital development offices and related foundations run programs in which donors have the opportunity to shadow physicians for a day in the health care facility. Such programs require patient authorization. Even if a donor signs a confidentiality agreement before participating and is instructed only to observe and not to interact with patients,

the HIPAA Privacy Rule includes no exemptions that allow donors to observe patient consultations or treatments *without patient's authorization*. Furthermore, when the patient is a minor, a shadow program must have authorization from the patient's parent(s) or other legal guardian(s).

Donor shadow programs differ from shadowing programs used for medical education and training. Under the HIPAA incidental disclosure rules, patient authorization is not required in order for medical students or other medical personnel to shadow physicians as they consult with and treat patients in compliance with the hospital's HIPAA policies; however, it is required for donor shadow programs.

Use of PHI in applying for grants

The HIPAA regulations provide no guidance on whether a development office or supporting foundation applying for a grant may derive general statistical information from patients' PHI without the patients' authorization. In the absence of guidance, AHP legal counsel's interpretation is that grant applications could be considered a form of fundraising if PHI is used in the application.

Under this interpretation, the development office or foundation could use patient demographic information and dates of service in compiling statistical data. Also, if the organization uses only de-identified patient information—data from which all information that could reasonably be used to identify the patient has been removed—in a grant application, no HIPAA concerns are present. Once patient information has been de-identified it is no longer protected by HIPAA since by definition it cannot be used to identify any patient. This is the preferred approach to minimize risk under HIPAA.

Soliciting long-term care patients' family members

Many long-term care providers solicit the family members of their residents, and long-term care providers that qualify as covered entities are subject to the HIPAA Privacy Rule. Names and contact information of family members obtained while providing treatment to a patient are demographic information and therefore can be used for fundraising purposes, assuming the appropriate Privacy Notice and communications opt-out provisions are followed.

Soliciting a health care provider's employees or a teaching hospital's alumni

HIPAA places no restrictions on the solicitation of employees or teaching hospital alumni, because the names and identifying information about these individuals are not PHI.

When in doubt...

Not sure if an activity or fundraising effort is in compliance? Apply the underlying tenet behind HIPAA—consider the minimum necessary patient data that is required to accomplish legitimate and necessary fundraising tasks. And then check with your hospital or health care organization privacy officer or legal counsel.



Notice of Privacy Practices

A Notice of Privacy Practices (Notice) is a formal written notice of a hospital's or health care provider's practices regarding the privacy of patient health information and of the rights of a patient regarding his or her personal health information (PHI). Every health care institution that has a direct treatment relationship with individuals must provide those individuals with copies of its Notice of Privacy Practices on their first service encounter so they are aware of how their information will be used and disclosed, including for any research, marketing and fundraising efforts. The health care provider must make a good faith effort to obtain each patient's written acknowledgement of having received a Notice of Privacy Practices. In the absence of a direct encounter, the patient's signed acknowledgement is not necessary.

NOTE: While your hospital or health care organization is responsible for the Notice, as a fundraiser, you should ensure that the Notice includes appropriate language regarding fundraising, since without it, you cannot contact patients for fundraising purposes. In the Preamble to the Modified Rule, OCR stated that the inclusion of the right to opt out is a material change to the Notice. The Privacy Rule requires certain actions whenever there is a material change to the Notice.

This section discusses

- › Required contents of a Notice of Privacy Practices
- › Availability of the Notice
- › Patient acknowledgement of the Notice

Required contents of a Notice

HIPAA imposes specific requirements regarding the contents of a Notice of Privacy Practices (NPP). Among them, the Notice must:

- › Be written in plain language.
- › Describe how individuals' protected health information (PHI) may be used and the limitations upon its use.
- › Include a statement describing the health care institution's policy and practices regarding soliciting individuals for funds.
- › Include a statement that the patient has the right to opt out of receiving any fundraising communications.
- › The right of affected individuals to be notified following a breach of unsecured protected health information.

NOTE: Because patients will be provided the opportunity to opt out of fundraising communications with each solicitation, the Notice of Privacy Practices does not need to describe a mechanism for patients to opt out of receiving fundraising communications.



A Notice of Privacy Practices must contain a separate statement that informs patients that the hospital may contact the individual to raise funds for itself and the individual has a right to opt out of receiving such fundraising communications. [45 CFR 520] You do NOT need to provide an opt-in or a description of how to opt-out as part of the Notice. To do so is a business decision, not a requirement under HIPAA.

Sample language

Example

We may use certain information (name, address, telephone number or e-mail information, age, date of birth, gender, health insurance status, dates of service, department of service information, treating physician information or outcome information) to contact you for the purpose of raising money for [Name of Entity] and you will have the right to opt out of receiving such communications with each solicitation. For the same purpose, we may provide your name to our institutionally related foundation. The money raised will be used to expand and improve the services and programs we provide the community. You are free to opt out of fundraising solicitation, and your decision will have no impact on your treatment or payment for services at [Name of Entity].

A health care provider may not use or disclose PHI in any way that is not mentioned in the Notice. If a hospital or health care provider Notice of Privacy Practices does not include language regarding fundraising and inform the patient that they will have the right to opt out from receiving such communications with each solicitation, then even the limited information permitted under HIPAA regulations *cannot* be used or disclosed to the development department or supporting foundation for fundraising efforts.

Availability of the Notice

The Notice of Privacy Practices must be made available to all patients. Among the requirements, the health care provider *must*:

- Post the Notice of Privacy Practices on its website and make it available electronically.
- Post the Notice in prominent places inside the institution's facilities.
- Have copies available for new patients or anyone who requests a copy.

The Notice may also be distributed through a health care provider's newsletter or other general communications vehicle.

A health care provider or supporting foundation is *not* required to mail the Notice of Privacy Practices to patients prior to sending them a fundraising solicitation. However, it must make a copy available (through its website, office postings, newsletters, etc.) prior to using even limited PHI for fundraising purposes, even if there is no direct opportunity or obligation to obtain an acknowledgement.

Patient acknowledgement of receiving the Notice

Only a health care provider with a direct relationship with patients must make a good faith effort to obtain an acknowledgement from the patient, but virtually all hospitals are within that category and subject to the requirement. The obligation must be fulfilled upon the health care provider's first in-person encounter with the patient, or upon any change to the Notice. Please contact your privacy officer to review what the Notice says about the steps the hospital will take to provide individuals with a revised Notice and follow those steps when there is a material change in the Notice.

Opt-out Provision

An opt-out provision is a statement, written or oral, provided to former patients that describes how they can discontinue receiving fundraising materials and solicitations from the health care provider or supporting foundation. HIPAA regulations mandate that an opt-out provision *must* be included with *each* fundraising communication or materials a health care provider or supporting foundation makes to former patients.

This section discusses

- › Opt-out requirements
- › Sample opt-out language
- › Use of languages other than English
- › Scope of the opt out
- › Expiration of the opt out
- › Non-written patient opt-out requests
- › Honoring patient opt-out requests
- › Opt-out requirements for invitations to special events
- › Inviting opted-out patients to special events
- › Opt-out requirements for newsletters and other general communication vehicles
- › Opt-out requirements for planned giving communications
- › Opt-out requirements once a patient becomes a donor
- › Penalties
- › Opt back in requirements

Requirements

All opt-out provisions made to patients must:

- › Be a clear and conspicuous part of the materials sent or stated orally to the patient.
- › Be written in clear, plain language. 
- › Describe a simple, not unduly burdensome means to opt out from receiving any further fundraising materials or communications.

NOTE: Like fundraising communications made in writing, phone solicitations must clearly inform patients that they have the right to opt out of further solicitations. The Modified Rule clarifies that the opt out requirement applies to fundraising communications “made” rather than “sent” to an individual.



Clear and plain language:

Changes made to HIPAA under HITECH require that the fundraising communication opt-out must be stated in a “clear and conspicuous manner.” [HITECH Act, Section 13406(b)] and the 2013 Modified Rule states that the hospital 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.” [45 CFR § 164.514(f)(2).] Plain language is mandated for the Notice; therefore, it is reasonable to infer that it applies to all patient communications. HHS defines plain language as information written in short sentences in the active voice, using common, everyday words. [Preamble 45 CFR § 164.520(b)]



Cannot cause undue burden:

Under the final rule, hospitals or institutionally related foundations are free to decide what methods patients can use to opt out as long as the opt-out method(s) does not result in undue burden or more than a nominal cost. Suggestions for the opt-out method included in the Preamble include:

- Toll-free and/or local telephone number.
- E-mail address.
- Pre-printed, pre-paid postcard
- Similar opt-out mechanism that is simple, quick and inexpensive.

Under the final rule, hospitals or institutionally related foundations are free to decide what methods patients can use to opt out as long as the opt-out method(s) does not cause undue burden or more than a nominal cost. Suggestions for the opt-out method include:

- Toll-free and/or local telephone number
- E-mail address
- Pre-printed, pre-paid postcard
- Similar opt-out mechanism that is simple, quick and inexpensive

Development offices or institutionally related foundations may use multiple opt-out methods or choose to use only one method. Requiring patients to write a letter to the development office or institutionally related foundation asking not to receive further fundraising communications is considered an undue burden and is not acceptable. If a written response is the preferred approach, the preferable opt-out method is to provide a pre-printed, pre-paid postcard.

NOTE: The final rule takes into account the expense of the opt-out methods, such as the use of a local and/or toll-free phone number, and clarifies the intent of not imposing an undue burden or cost on the individual. Development offices or institutionally related foundations are encouraged to take into account which opt-out methods are most appropriate and least burdensome to individuals. Factors to consider include the size of population receiving the fundraising communications or the geographic distribution.

Sample language

Example

If you do not want to receive future fundraising requests supporting [Name of Entity and/or name of specific campaign], please check the box on the enclosed printed, pre-addressed and pre-paid card and drop in the mail. As an alternative, you can call our telephone number [either the local number [list] or our toll free number [list] and leave a message identifying yourself and stating that you do not want to receive fundraising requests. There is no requirement that you agree to accept fundraising communication from us, and we will honor your request not to receive any [more altogether or more with respect to the identified campaign] fundraising communications from us after the date we receive your decision.

Languages other than English

HIPAA regulations do not outline requirements for providing opt-out statements in multiple languages, but the discussion in the Preamble to the Modified Rule advises that it may be necessary depending on the patient population served. The language requirements that pertain to other areas of health care communication (e.g., Notices of Privacy Practices) do not specifically apply to opt-out provisions, but the better course is to consider the demographics of your target population in considering the need to account for limited English proficiency recipients. If the fundraising solicitation being sent to patients is multilingual, the opt-out provision in each of the languages of the solicitation must be included.

Scope of the opt-out

The final rule leaves the scope of the opt-out to the discretion of the hospital, through its development office or institutionally related foundation. At the direction of the hospital, which is the covered entity, development offices or institutionally related foundations may provide patients with the choice of opting out of all future fundraising communications or just campaign-specific communications. Whatever method is used, the opt-out should clearly inform patients of their options and any consequences of electing to opt out of further fundraising communications.

Expiration of the opt-out

A patient's election not to receive further fundraising communications does not lapse unless they affirmatively opt back in. Because the patient has actively chosen to opt out, only a similar active decision to opt back in will suffice. Additionally, the Preamble states that when an individual who has opted out of fundraising communications makes a donation, it does not serve, absent a separate election to opt back in, to automatically add the individual back into the mailing list for fundraising communications.

Non-written patient opt-out requests

Many health care providers would prefer that patients submit their opt-out requests in writing. However, current HIPAA regulations do not require that patient opt-out requests be written, unless the method chosen does not impose a burden on the patient. (If a written request is chosen, it should be a pre-printed, check the box, pre-addressed and pre-paid card the recipient merely has to drop in the mail.) If the recipient has elected to receive all communications electronically, that request should be honored. Of course, electronic communications cannot be the only option because many patients may lack access, but it can be included as an option together with local and toll free numbers. Hospitals should carefully consider the intended recipients of fundraising communications and design an opt-out alternative that is both compliant and which can be monitored and enforced.

The Privacy Rule is intended to balance the individual's need and expectation for protection of their health information against the health care provider's legitimate requirements to function properly.

Honoring patient opt-out requests

Hospitals and health care providers are *required* to honor a patient's request to no longer receive fundraising communications. While the HIPAA Privacy Rule originally stated that covered entities must make a "reasonable effort" to ensure that individuals who opt out are not sent further fundraising communications, changes to the Privacy Rule make compliance a *statutory requirement*. The hospital, or its development office or institutionally related foundation, is responsible for honoring all such requests, and for designing a system that it can manage. If, for example, toll-free and local telephone lines are chosen, they must be checked often and routinely, with an effective system to enforce the requirement. If oral contacts will be made, it is not enough to simply delete names from mailing lists. 



Honoring patient opt-out requests:

"When an individual elects not to receive any further such communication, such election shall be treated as a revocation of authorization under section 164.508 of title 45, Code of Federal Regulations." [HITECH Act, Section 13406 (b)] The Modified Rule states that the hospital "may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications." [45 CFR § 164.514(f)(2).]

Opt-out provisions and invitations to special events

If a health care provider stages special events for grateful patients and donors and the invitation includes a “donation per plate” or other fundraising request, the invitation should include or be accompanied by an opt-out provision. If no fundraising is involved, no opt-out language is required.

Inviting opted-out patients to educational events

HIPAA regulations do not address situations where *educational events* contain active or passive fundraising. AHP legal counsel’s interpretation is that a hospital or health care provider can send an individual who has opted out from receiving fundraising communications information about educational and other events that it sponsors. However, if active fundraising is part of the program, an opt-out provision must be included.

Newsletters, brochures and general audience communications

Newsletters and other types of fundraising and marketing communications intended for *educational* purposes for a general audience that includes former patients do not have to include opt-out language. However, if the newsletter or communications piece contains a fundraising appeal or if a return envelope intended for donations is included, an opt-out provision is required. Since failure to include an opt-out with any fundraising communication is a violation of the Privacy Act, the Privacy Officer should be consulted if there is any doubt. The Preamble to the Modified Rule included the following description of fundraising communications:

A communication to an individual that is made by a covered entity, an institutionally related foundation, or a business associate on behalf of the covered entity for the purpose of raising funds for the covered entity is a fundraising communication for purposes of § 164.514(f). The Department has stated that “[p]ermissible fundraising activities include appeals for money, sponsorship of events, etc. They do not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc.).”

Planned giving communications

If a health care provider or related foundation uses a patient mailing list to send out newsletters, letters or brochures with information about planned giving, or a planned giving event, with a response card or mechanism for requesting more information, the mailing may be considered purely educational and not fundraising. However, if the planned giving is for the benefit of the hospital, health care organization or related foundation, including an opt-out ensures there is no inadvertent violation of the HIPAA Privacy Rule.

NOTE: A general communication about planned giving sent to a patient listing that is not for the benefit of the institution may be considered marketing if the event encourages patients to use the services of a financial planning or estate planning individual or group. HIPAA limits use of patient information for marketing purposes without patient authorization (see page XX). If the covered entity receives any compensation for something considered marketing, with limited exceptions, it cannot use any PHI (including the type of data permitted for fundraising) for the effort, including names and addresses of patients, without authorization.

Opt-out requirement once a patient becomes a donor

HIPAA does not distinguish between former patients and former patients that have become donors; therefore, you should provide opt-out language in every fundraising communications to *all* former patients, whether they have become donors or are still prospective donors. Additionally, when an individual who has opted out of fundraising communications makes a donation, it does not serve, absent a separate election to opt back in, to automatically add the individual back into the mailing list for fundraising communications.

Penalties for not honoring opt-out requests

Failure to honor opt-out requests are considered to be the same as failing to comply with revocations of authorizations, and constitute violations of the Privacy Rule. The covered entity – the hospital – is responsible for devising a system that it can enforce given its limitations.

Opt-in requirement

A health care provider or its related foundation may, but is not required to, create a workable solution to permit those who have opted out to opt back in. As with the case of the opt-out itself, the process must be clear and simple. The Modified Rule does not provide further specifics to the opt-in process. However, since an election to opt out is considered under the statute as the same as a revocation for authorization, any opt in process must be absolutely clear. Our recommendation is that it should involve a written and signed document specifically electing to revoke the signer's prior election to opt-out in clear and conspicuous language, since such a statement would be required for an authorization.

Fundraising Vendor and Business Associate Agreements



Definition of an institutionally related foundation:

The 2013 Modified Rule does not define the term but in a prior Preamble HHS commented that it is a "foundation that qualifies as a nonprofit charitable foundation under Sec. 501(c)(3) of the Internal Revenue Code and that has in its charter statement of charitable purposes an explicit linkage to the covered entity. An institutionally related foundation may, as explicitly stated in its charter, support the covered entity as well as other covered entities or health care providers in its community."

HIPAA recognizes that a health care provider may have relationships with other entities and vendors that perform health care operations services on its behalf, and outlines requirements to ensure the protection of patient information in these instances through the use of business associate agreements (BAAs). This does not, however, apply to the relationship between a health care provider and its institutionally related foundation.

This section discusses

- › Important terms
- › Distinction between an institutionally related foundation and a business associate
- › Use of BAAs and fundraising vendors and consultants
- › Use of BAAs and volunteers
- › BAA specifics
- › Business associate liabilities
- › Applicability to subcontractors

Important terms

Fundraising vendor: A private company or fundraising services provider that is not directly related to the health care provider or its health care operations but instead functions under contract to support the health care provider's operations.

Institutionally related foundation: A nonprofit corporation, foundation, institute or similar entity that is organized for the benefit of one or more covered entities. Its principal purpose is to receive or use private donations for medical or health care related programs or services conducted by the covered entities.

Business associate: Any person or entity that provides certain services to or for a health care provider that involve the disclosure of protected health information or any person or entity that creates, receives, maintains, or transmits protected health information for certain functions or activities on behalf of a health care provider. A subcontractor of a business associate who creates, receives, maintains, or transmits PHI on behalf of the business associate also is now a business associate. A more in-depth definition is found in Appendix A.

Subcontractor: A person to whom a business associate has delegated a function, activity, or service the business associate has agreed to perform for a covered entity or business associate (other than in the capacity of a member of the workforce of such business associate).



Business associate agreement (BAA): A formal written agreement between a health care provider and each of its business associates and between a business associate and a business associate that is a subcontractor. The agreement must (among other things):

- Describe the permitted and required uses of protected health information by the business associate (or subcontractor, as applicable);
- Provide that the business associate (or subcontractor, as applicable) will not use or disclose any protected health information other than as permitted or required by the contract or by law;
- Require the business associate (or subcontractor, as applicable) to use appropriate safeguards and comply, where applicable, with the Security Rule, with respect to electronic protected health information, to prevent any use or disclosure of protected health information other than as provided for by the contract;
- Require the business associate (or subcontractor, as applicable) to report any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by the Breach Notification Rule; and
- Provide for the destruction or return of any PHI at the termination of the contract, or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

Note: Covered entities must ensure that they obtain satisfactory assurances from their business associates that such business associates will appropriately safeguard the PHI and ePHI at issue, and business associates must do the same with regard to subcontractors, and so on, no matter how far “down the chain” the information flows. The covered entity—the hospital—does not have to have a BAA with such subcontractors, but the business associate must itself obtain satisfactory assurances from its subcontractors. The Privacy and Security Rules state that satisfactory assurances are obtained by entering into a valid BAA. Therefore, the hospital must enter into a BAA with its business associate, and the business associate should enter into a BAA with its subcontractors requiring it to comply with the limitations imposed by the hospital on its business associate, and so on down the line. We suggest that the hospital’s BAA require the business associate to enter into a BAA with each subcontractor that will receive or use PHI from the hospital or its institutionally related foundation and that the hospital require its business associates to provide the hospital with the contact information of business associate’s subcontractors and a copy of the BAAs between business associate and its subcontractors.

Distinction between an institutionally related foundation and a business associate

Although HIPAA regulations do not define a distinction between an institutionally related foundation and a business associate, the regulations consistently identify the two separately.

A hospital or health care organization is *NOT* required to have a business associate agreement with its institutionally related foundation, because the regulations consider such a foundation part of the entity’s health care operations. HHS clarified in its April 2, 2003



BAA contracting parties:

The business associate agreement required by HIPAA must be between the hospital or health care organization (covered entity) and the vendor, even if the institutionally related foundation has the contractual relationship with the fundraising vendor or consultant. If the business associate uses subcontractors, it, but not the hospital or health care organization, must have a BAA or similar document with each subcontractor.

letter to AHP that the HIPAA Privacy Rule permits disclosures of patient information for fundraising purposes to institutionally related foundations without a business associate agreement. (See Appendix D.)

In its Preamble, the HIPAA Privacy Rule indicates that a health care provider can disclose patient information to an institutionally related foundation if the provider either:

- Includes the foundation in its Notice of Privacy Practices,
- Enters into a business associate agreement with the foundation, or
- Relies on the Preamble language.

Whichever approach the health care provider takes, the organization performing fundraising duties on behalf of the provider must meet the definition of an institutionally related foundation. 

Almost all traditional nonprofit fundraising entities affiliated with health care providers, which are generally formed as supporting organizations under Section 509(a)(3) of the Internal Revenue Code, or as public charities under Section 509(a)(1), are considered institutionally related foundations, even if the supporting health care provider is not the only recipient of its support.

HHS has concluded, however, that the term does not include an organization with a general charitable purpose, such as to support research about or to provide treatment for certain diseases, which may give money to a health care provider. This is because the organization's charitable purpose is not specific to or supportive of the health care provider. Although this distinction is critical, it generally does not impact traditional hospital and health care provider foundations.

Fundraising vendors and business associate agreements

A hospital or health care organization must have a business associate agreement with a fundraising vendor if:

- The fundraising vendor or consultant is not part of the health care provider or its institutionally related foundation, and
- Patient information will be released to the entity.

A health care organization must enter into a business associate agreement with any consultant it or its supporting foundation retains, if the consultant is provided access to patient information. Although business associates are now directly liable under the HIPAA rules for impermissible uses and disclosures, business associate agreements give health care providers some degree of protection – satisfactory assurances – should the business associate fail to comply with the Privacy Rule. The health care provider, however, must take reasonable corrective action or terminate the contract if it learns that the business associate is not in compliance. (*See the discussion of BAA on page XX.*) Consultation with your privacy officer with respect to all such contracts is recommended.

Volunteers and business associate agreements

Volunteers, including board members, working with the development office or related foundation on fundraising activities, and who have access to permissible patient information, are defined as “part of the workforce.” Regulations do *not* require the health care provider to have a business associate agreement with them individually, although they must receive the entity’s HIPAA training. 

HIPAA business associate agreement specifics

Development offices and related foundations must ensure that any vendor or consultant with which they contract that has access to or uses patient information has a current and compliant business associate agreement in place with the hospital or health care provider. The agreement should include the vendor’s obligations for HIPAA compliance in using or disclosing patient information and responsibilities in reporting disclosures or breaches.

An annotated sample HIPAA business associate agreement is provided in Appendix C. This sample agreement provides both required and suggested information to include in an agreement that would be attached as an addendum to the underlying contract with a business associate and is *modeled after the sample document released by the Office of Civil Rights*. Recommendations and explanations are provided throughout the sample agreement. You should contact your hospital or health care provider privacy officer regarding business associate addendums and should not adopt this BAA without first consulting with legal counsel.

Business associate and subcontractor liability

Under the original HIPAA regulations, business associates were not directly subject to HIPAA, and their responsibilities and liabilities were the result of their contract with the hospital or health care provider. The HITECH Act of 2009 changed this. Now, business associates and their subcontractors (who are also “business associates” under the Modified Rule) are directly liable under the HIPAA Rules for impermissible uses and disclosures, for a failure to provide breach notification to the covered entity, for a failure to disclose protected health information where required by the Secretary to investigate or determine the business associate’s compliance with the HIPAA Rules, and for a failure to comply with the requirements of the Security Rule. Depending on the language in the BAA, it may also be responsible for a failure to provide access to a copy of electronic protected health information to the covered entity, the individual, or the individual’s designee, for a failure to provide an accounting of all disclosures, or for other requirements contained in the BAA. The minimum necessary standard applies to business associates when using or disclosing protected health information. Under the Security Rule, the only two permissible methods to protect PHI are encryption, destruction, or return of all of the PHI disclosed. Please consult your privacy officer with respect to these issues. 



As a best practice, the development organization should train all volunteers on HIPAA requirements and the processes and procedures to ensure protection of patient information, and maintain records of such training. As members of the workforce of the hospital or health care organization, such training is required.



HITECH changes to BAA:

Fundraisers should ensure that all business associate agreements between their vendors and health care organization comply with the changed requirements for a BAA. There are special rules with respect to when a BAA must be amended to comply with the Modified Rule, and restrictions on renewals without amendment apply. Consult the Privacy Officer of your hospital or health care organization to ensure compliance.

Marketing and the Privacy Rule



Marketing defined:

Marketing is (with very limited exceptions) any communication about a product or service that encourages recipients of the communication to purchase or use the product or service. [45 CFR § 164.501]

While the focus of this guide is fundraising, it is important for development organizations, institutionally related foundations and their business associates to understand and comply with HIPAA restrictions regarding marketing efforts. The HIPAA Privacy Rule requires patient authorization for the use of *any* patient protected health information (PHI) in connection with marketing, except for face-to-face communications made by the hospital to the individual and use of promotional gifts with a nominal value.

This section discusses

- › Definition of marketing
- › Distinction between marketing and other activities
- › Avoiding potential HIPAA violations related to marketing materials

Definition of marketing

The HIPAA Privacy Rule defines marketing as any communication about a product or service that encourages recipients to purchase or use the product or service unless the product or service is provided by the covered entity (hospital or health care provider). Patient authorization is required in order to use PHI for marketing efforts.

A communication does NOT require patient authorization, even if it may be marketing, in the following two exceptions only:

- › When the communication is being made face-to-face by a health care provider to an individual.
- › The health care provider is providing a promotional gift of nominal value, such as giving new mothers, as they leave the maternity ward, a free package of formula and other baby products.

HITECH made significant changes to the HIPAA legislation in this area, including adding large penalties for inappropriate use or disclosure of patient information in connection with marketing. The American Recovery and Reinvestment Act of 2009, of which HITECH is a part, also prohibits a hospital or health care provider from receiving direct or indirect compensation or remuneration in exchange for patient information, without the patient's authorization, with some limited exceptions.

NOTE: Fundraising is **NOT** considered marketing. The two are separately discussed in the HIPAA legislation and regulations, and fundraising is defined as part of health care operations. HIPAA also forbids the sale of PHI in general without authorization.



Distinction between marketing and other activities

The following guidelines help distinguish between marketing and other communications and informational activities:

Marketing

A newsletter, flyer, email, social media contact or other communication is likely to be considered marketing if it is about a product or service that encourages recipients of the communication to purchase or use a product or service that is *not* provided by the health care provider, or if the provider received any remuneration for making the communication.

Examples

- A flyer is sent to a listing of former cardiology patients promoting a new drug available through a pharmaceutical company.
- A health care provider, in exchange for remuneration, provides a listing of patients to a drug manufacturer, who in turn contacts the patients directly regarding a new medication.

Not marketing

A newsletter, flyer, email, social media contact or other communication is generally not considered marketing if it merely describes the services and products that a *health care provider offers, and the provider has not been reimbursed for making the communication*. Therefore, a provider may use a PHI-derived mailing list to send patients materials listing its products or services, to announce changes to its offerings, or announce or recommend its available alternative treatments, therapies, health care providers or settings of care as long as it was not reimbursed to make the communication.

Examples

- A notice or article is sent to former patients announcing the opening of a new hospital orthopedic or pediatric department, or the acquisition of a new technology.
- A flyer announcing a hospital's new weight-loss program, is sent to all patients seen by the provider who were defined as obese, even if their treatment received was not specifically for obesity.

Avoiding risk in marketing

Hospitals, health care organizations and their fundraising departments or institutionally related foundations can minimize the risk of using PHI for prohibited marketing purposes by avoiding the use of mailing lists that are derived from patient lists for newsletters and other mailings *that contain marketing messages, and by failing to accept remuneration for marketing any products*.

Breaches, Notification and Penalties



Instructions for submitting a notice of breach and the online submission form can be found on the HHS website at: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

In the case that there is an unauthorized disclosure of patient protected health information (PHI), HIPAA outlines requirements for notification to the patient, media and HHS, as well as penalties for such a breach. While the health care organization is responsible for establishing the internal processes and procedures for reporting breaches and will handle any mitigation required in the case of a breach, fundraisers should be aware of their and their vendor's responsibilities.

This section discusses

- Definition of a breach
- Requirements for notification of a breach
- Penalties for breaches

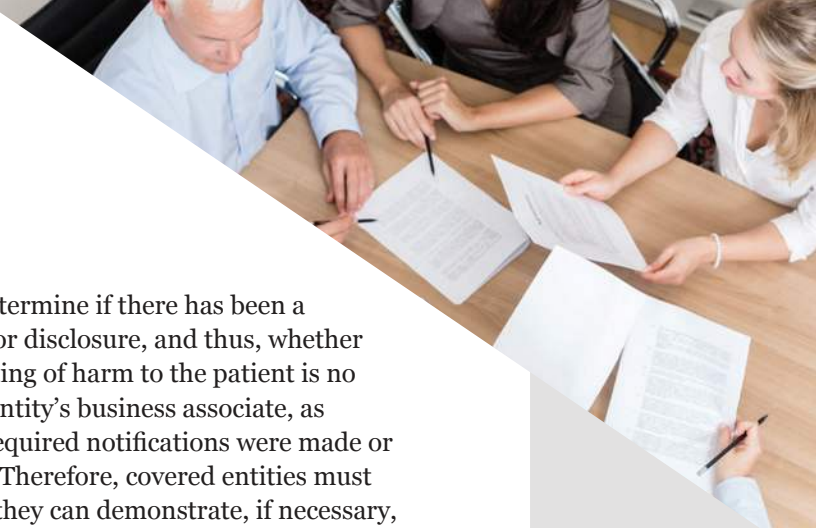
Definition of a breach

HIPAA previously defined a breach as an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of patient protected health information such that the use or disclosure poses a significant risk of financial, reputational or other harm to the affected individual. The Modified Rule made a substantive change in this definition, described below, that is effective on September 23, 2013. Breaches that occur before that date are still governed by the current rule.

Health care providers and business associates must provide notification only if the breach involves *unsecured* protected health information. Unsecured protected health information is data that has *not* been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology such as encryption or by destruction. All other PHI is unsecured.

There are three *exceptions* to the breach definition:

1. Unintentional acquisition, access or use of protected health information by a workforce member acting under the authority of a health care provider, supporting foundation or business associate, where the information is not further used or disclosed in a manner not permitted by the Privacy Rule.
2. Inadvertent disclosure of protected health information from a person authorized to access protected health information at a health care provider, supporting foundation or business associate to another person authorized to access protected health information at the health care provider or business associate, where the information is not further used or disclosed in a manner not permitted by the Privacy Rule.
3. Where a health care provider, supporting foundation or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.



Required risk assessment

Covered entities must perform a risk assessment to determine if there has been a disclosure of PHI as a result of the impermissible use or disclosure, and thus, whether there has been a “breach.” The prior standard of a finding of harm to the patient is no longer applicable. The covered entity (or the covered entity’s business associate, as applicable) has the burden of demonstrating that all required notifications were made or that the use or disclosure did not constitute a breach. Therefore, covered entities must perform and document their risk assessments so that they can demonstrate, if necessary, that no breach notification was required.

Under the rules in effect until September 23, 2013, the definition of “breach” requires a review of whether a significant risk of financial, reputational, or other harm to the individual is likely to occur as a result of the impermissible use or disclosure, and thus, whether there has been a “breach.” The covered entity (or the covered entity’s business associate, as applicable) has the burden of demonstrating that all required notifications were made or that the use or disclosure did not constitute a breach. Therefore, covered entities must document their risk assessments so that they can demonstrate, if necessary, that no breach notification was required.

The required risk assessment should consider a number or combination of factors, including (but not limited to) the following:

- Who impermissibly used the information or to whom the information was impermissibly disclosed.
- Whether immediate steps were taken to mitigate an impermissible use or disclosure, such as by obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed.
- Whether the impermissibly disclosed PHI is returned prior to it being accessed for an improper purpose.
- The type and amount of PHI involved in the impermissible use or disclosure.

By doing a risk assessment, entities may determine that the risk of identifying a particular individual is so small that the use or disclosure poses no significant risk of harm to any individuals. If there is no significant risk of harm to the individual, no breach has occurred and no notification is required. If, however, the entity determines that the individual can be identified based on the information disclosed, and there is otherwise a significant risk of harm to the individual, breach notification is required (unless one of the other exceptions applies).¹

Subsequent to September 23, 2013, the definition of breach is changed to include any improper disclosure of PHI, unless one of the three exceptions applies. If after that date the risk assessment indicates that a breach occurred—even a disclosure that is not likely to harm the patient – the notice and penalty requirements apply.

¹A covered entity or business associate is not responsible for a breach by a third party to whom it permissibly disclosed PHI unless the third party received the information in its role as an agent of the covered entity or business associate. If a third party recipient of the information is a covered entity and the information is breached while at the third party, the third party is responsible for complying with the Breach Notification Rule.



As a best practice, work with your hospital or health care organization privacy officer and document for your development organization and vendors definitions and examples of breaches, and the process and timeframes for reporting breaches.

Notification of breach requirements

A covered entity that discovers a breach of unsecured protected health information (PHI), as those terms are defined below, must make the following notifications:

1. The covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. 
2. If the breach involves more than 500 residents of a state or jurisdiction, a covered entity must notify prominent media outlets serving the state or jurisdiction.
3. The covered entity must also notify the Secretary of the Department of Health and Human Services (the “Secretary”).
 - For breaches involving 500 or more individuals, this notice must be contemporaneous with the notice to individuals.
 - For breaches involving less than 500 individuals, the covered entity must maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, notify the Secretary of breaches occurring during the preceding calendar year.

Health care providers and business associates are required to disclose a privacy breach to the individuals affected and to the Secretary of HHS as soon as possible but no later than 60 days following the *discovery* of a breach. A breach is discovered when the covered entity or its business associate learned, or through the exercise of reasonable diligence should have learned, about its existence².

Notice to individuals

Notice to individuals must be in written form by first-class mail, or by email if the affected individual has agreed to receive notices electronically, and must include a description of the breach, a description of the types of information that were involved in the breach, the steps the individual should take to protect themselves from potential harm, a description of what the health care provider is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the health care provider.

Notice to media

For a breach affecting more than 500 residents of a state or jurisdiction, in addition to notifying the affected individuals, a health care provider or business associate is required to provide notice to prominent media outlets serving the state or jurisdiction.

²Note that delays by a business associate or institutionally related foundation in providing breach notification create significant problems for the hospital.

Notice to the HHS Secretary

Health care providers and business associates must notify the Secretary of HHS regarding breaches of unsecured protected health information by visiting the HHS website and submitting the online breach report form as follows: For breaches affecting 500 or more individuals, notification must be made no later than 60 days following the breach. For breaches affecting fewer than 500 individuals, notification may be made on an annual basis no later than 60 days after the end of the calendar year in which the breach(es) occurred.

Penalties

The HITECH Act of 2009 strengthened the HIPAA Enforcement Rule by creating four categories of violations that reflect increasing levels of culpability with associated tiered penalty levels, with a maximum penalty of \$1.5 million for all violations of an identical provision within one year. In addition, state attorneys general are authorized to take civil action against health care providers and business associates regarding breaches of patient information. The FTC also has been granted enforcement authority against organizations that are not directly subject to HIPAA. The penalty provisions leave large amounts of discretion to the federal government, except that the Modified Rule essentially eliminated the discretion not to impose any penalty at all for a breach. Since the issue now is simply whether a disclosure other than one of the limited exceptions occurred, and the previous discretion has been removed, all breaches will lead to some sort of penalty.

NOTE: HITECH requires a business associate of a covered entity that accesses, maintains, retains, modifies, records, destroys or otherwise holds, uses or discloses unsecured protected health information to notify the covered entity when it discovers a breach of such information. Business associates must provide such notification to covered entities without unreasonable delay and in no case later than 60 days from the discovery of the breach.

Appendix A—Definitions

Authorization. A detailed document that gives a health care provider permission to 1) use a patient's protected health information for specified purposes other than treatment, payment, or health care operations, or 2) disclose protected health information to a third party specified by the individual. An authorization must:

- Describe the protected health information to be used or disclosed in a specific and meaningful fashion;
- Identify the person or entity authorized to make the use or disclosure;
- Identify the person or entity to which the health care provider may make the use or disclosure;
- Include an expiration date;
- Describe the purpose(s) for which the information may be used or disclosed;
- Include the individual's signature and date and a description of a personal representative's authority to act for the individual if applicable; and
- Contain certain specified statements adequate to place the individual on notice of certain elements.

A covered entity may not condition the provision to an individual of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization except under certain circumstances. Additionally, a covered entity cannot make decisions about patient treatment or coverage based on the individual's choice regarding the receipt of fundraising communications or the patient's decision to authorize, or not authorize, use of their information for fundraising.

Breach. The acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule which compromises the security or privacy of the protected health information. Breaches exclude:

- Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule;
- Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or
- A disclosure of PHI where a covered entity or business associate 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.

Business Associate. A business associate is any person or entity that creates, receives, maintains, or transmits protected health information on behalf of a covered entity for a function or activity regulated by the HIPAA rules. It also includes any person or entity that provides services to or for a covered entity involving the disclosure of protected health information. Business associate services include legal, actuarial, accounting, consulting, data aggregation, management, data transmission, administrative, accreditation, financial or personal health record services. Business associate functions or activities include claims processing or administration; data analysis, processing, or administration; direct mail and mail house functions; utilization review; quality assurance; certain patient safety activities; billing; benefit management; practice management; and repricing. A subcontractor of a business associate who creates, receives, maintains, or transmits PHI on behalf of the business associate is now a business

associate (although the business associate, not the covered entity, has an obligation to enter into a business associate agreement with the subcontractor). There are certain exceptions from the definition of business associate, including a covered entity participating in an organized health care arrangement (OHCA) that performs one of the above-described activities or functions for on or behalf of such OHCA or that provides one of the above-described services to or for such OHCA by virtue of such activities or services.

Business Associate Agreement. The formal written agreement that the HIPAA rules require between a health care provider (covered entity) and each of its business associates and between a business associate and a business associate that is a subcontractor. Among other things, the agreement must:

- Describe the permitted and required uses of protected health information by the business associate (or subcontractor, as applicable);
- Provide that the business associate (or subcontractor, as applicable) will not use or disclose any protected health information other than as permitted or required by the contract or by law;
- Require the business associate (or subcontractor, as applicable) to use appropriate safeguards and comply, where applicable, with the Security Rule with respect to electronic protected health information, to prevent any use or disclosure of protected health information other than as provided for by the contract;
- Require the business associate (or subcontractor, as applicable) to report any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by the Breach Notification Rule; and
- Provide for the destruction or return of any PHI at the termination of the contract, or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

A sample HIPAA business associate agreement that can be added to an existing vendor agreement can be found in Appendix C.

Covered Function. A function of a covered entity that makes the entity a health plan, health care provider or health care clearinghouse.

Covered Entity. A health plan, health care clearinghouse or health care provider who, in connection with transactions covered by the Privacy Rule, transmits any health information in electronic form.

De-identified Information. Health information from which all information that could reasonably be used to identify the patient has been removed including name, address, SSN, dates, telephone numbers, fax numbers, email addresses, medical record numbers, account numbers, etc. Once information has been de-identified, it is no longer protected health information protected by HIPAA and can be used for any purpose.

Disclosure. The release, transfer, provision of access to, or divulgence in any manner of information outside the entity holding the information.

Electronic Media.

- Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.
- Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Health Care. Care, services or supplies related to the health of an individual. Health care includes, but is not limited to:

- Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care.
- Counseling, services, assessments or procedures related to the physical or mental condition or functional status of an individual or that affect the structure or function of the body.
- Sale or dispensing of drugs, devices, equipment or other items in accordance with prescriptions.

Health Care Clearinghouse. A public or private entity that either:

- Receives from another entity health information in a nonstandard format or containing nonstandard data content and processes or facilitates the processing of that information into standard data elements or a standard transaction; or
- Receives from another entity a standard transaction and processes or facilitates the processing of the health information into nonstandard format or nonstandard data content for the receiving entity.

Health care clearinghouses include billing services, repricing companies, community health management information systems, community health information system and “value-added” networks and switches.

Health Care Operations. Certain administrative, financial, legal and quality improvement activities necessary to operate a health care provider’s business and support the core functions of treatment and payment. HIPAA defines fundraising for the benefit of the covered entity as a part of a health care provider’s health care operations.

Health Care Provider. An individual or organization that furnishes, bills, or is paid for health care in the normal course of business. Health care providers that only transmit information and do billing using non-electronic (including FAX) methods are not considered covered entities.

Health Information. Any information, including genetic information, whether oral or in recorded form or medium that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, educational institution or health care clearinghouse; and
- 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.

HHS. The U.S. Department of Health and Human Services. Within HHS, the Office of Civil Rights (OCR) has responsibility for enforcing the HIPAA rules.

Individual. A person who is the subject of protected health information.

Individually Identifiable Health Information (IIHI). A subset of health information, including demographic information collected from an individual, and which:

- Is created or received by a health care provider, health plan, employer or health care clearinghouse; and
- 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; and that either
 - Identifies the individual, or
 - Provides a reasonable basis for the belief that the information could be used to identify the individual.

Institutionally Related Foundation. A foundation that qualifies as a nonprofit charitable foundation under § 501(c)(3) of the Internal Revenue Code and has in its charter statement of charitable purposes an explicit linkage to the health care provider. An institutionally related foundation may, as explicitly stated in its charter, support the health care provider as well as other covered entities or health care providers.

Marketing. Communicating about a product or service in a way that encourages the recipients of the communication to purchase or use that product or service. Marketing does not include a communication made:

- To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.
- For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:
 - For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;
 - 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, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
 - For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Minimum Necessary Standard. The requirement that covered entities and business associates evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. The HIPAA Privacy Rule requires a health care provider and business associate to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish legitimate tasks. Disclosures (and requests for disclosures) between health care providers for treatment purposes are among the exemptions from the minimum necessary standard.

Notice of Privacy Practices (Notice). The formal written notice of a health plan's or health care provider's practices regarding the privacy of patient health information and of the rights of a patient regarding his or her personal health information (PHI). The HIPAA Privacy Rule requires health plans and covered health care providers to develop and make available a notice of privacy practices that clearly explains their privacy practices and their patients' rights. The Notice is intended to focus patients on privacy issues and encourage them to exercise their rights and discuss their concerns with their health plans and health care providers.

Organized Health Care Arrangement (OHCA). Includes, among others, one of the following:

- A clinically integrated care setting in which individuals typically receive health care from more than one health care provider.
- An organized system of health care in which more than one covered entity participates and in which the participating covered entities:
 - Hold themselves out to the public as participating in a joint arrangement; and
 - Participate in joint activities that include at least one of the following:
 - ◇ Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
 - ◇ Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
 - ◇ Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
- Other OHCA's involve certain group health plans and, in some cases, health insurance issuers or HMOs.
- **Payment.** Various activities of:
 - Health care providers to obtain reimbursement for their services.
 - Health plans to:
 - Obtain premiums or to determine or fulfill their responsibilities for coverage and provision of benefits under the health plan (except as otherwise prohibited); or
 - Obtain or provide reimbursement for the provision of health care.

Privacy Officer. The person designated by the health care provider to develop, implement and oversee the entity's compliance with the HIPAA Privacy Rule. The privacy officer may also serve as the entity's contact person for privacy issues. A hospital or health care organization (covered entity) is required to appoint a privacy officer.

Protected Health Information (PHI). Individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Electronic protected health information means information that comes within the first two bullet points. Protected health information excludes the following individually identifiable health information:

- in educational records covered by the Family Educational Rights and Privacy Act (FERPA);
- in records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
- in employment records held by a covered entity in its role as employer; and
- regarding a person who has been deceased for more than 50 years.

Required By Law. A mandate contained in law that is enforceable in a court of law, which compels an entity to use or disclose protected health information. Required by law includes, but is not limited to:

- Court orders and court-ordered warrants;
- Subpoenas or summons issued by a court, a grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information;
- A civil or an authorized investigative demand;
- Medicare conditions of participation with respect to health care providers participating in the Medicare program; and
- Statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Secretary. The Secretary of the U.S. Department of Health and Human Services or his or her designee.

Subcontractor. A person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

TPO. Treatment, payment and health care operations. Under HIPAA regulations, fundraising is a part of health care operations.

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 care provider to another.

Unsecured Protected Health Information. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of HITECH.

Use. With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Appendix B—Sample Patient Authorization Form

This sample Authorization for Use or Release of Health Information is published by the Association for Healthcare Philanthropy. It is not intended to provide legal advice or opinion. Entities should consult with legal counsel in reviewing and creating their own authorization form and should not adopt this form without first consulting with legal counsel. This form is drafted in light of the law and regulations as they exist as of March 1, 2012.

AUTHORIZATION FOR USE OR RELEASE OF HEALTH INFORMATION

I hereby voluntarily authorize the use of or release of my health information to [Name of Entity] to permit [Name of Entity] to use or disclose the identified health information in connection with or in furtherance of the [Name of entity] fundraising efforts, as follows:

I. Individual Information

Name: _____

Address: _____

Phone: _____

II. Identification of Person or Organization Receiving Information

My health information may be disclosed to the following organization(s):

[Name of entity]

[Address]

[Phone]

III. Purpose(s) for the Release or Disclosure of Information

- ☐ For the purpose of raising funds, or soliciting funds, or targeting the solicitation of funds, for and in furtherance of the activities of [Insert name of supported entity]

IV. Description of Information to be Released or Disclosed (check all appropriate)

- ☐ Patient records
- ☐ Diagnosis and treatment received while a patient at the [insert name of entity]

Exclusions (please specify):

- ☐ I request that the following information not be used or disclosed in connection with the fundraising efforts described above: _____

V. Other Important Information

Your signature below means that you understand and agree to the following:

- The health information provided under this authorization may include diagnosis and treatment information, including information pertaining to chronic diseases, behavioral health conditions, alcohol or substance abuse, communicable diseases (including HIV/AIDS), and/or genetic marker information. These records may be included in the information we will make available to the individual or organization you have identified above.
- The information to be disclosed may be protected by law. Information disclosed under this authorization may be redisclosed by the recipient and no longer protected by federal privacy regulations.
- You must sign this form in order for your request to release the information described above to be honored.
- You may receive a copy of this form if you ask for it by writing to the provider.
- This authorization will expire two years from the date you sign this authorization.
- If you sign this form, you may revoke the authorization at any time by notifying, in writing, the provider who is disclosing the information. Revoking this authorization will not have any effect on actions taken in reliance on the authorization before notice is received of your revocation.

VI. Signature of Individual or Individual's Representative

Signature of individual or representative

Date

If this authorization is signed by an individual's representative, the following additional information must be provided:

Name of personal representative (please print)

Relationship to the individual, including authority for status as representative

Appendix C—Sample HIPAA Business Associate Agreement

This sample Business Associate Agreement (BAA) is published by the Association for Healthcare Philanthropy. It is intended to be attached to the underlying agreement with the business associate. It has been written for contracts between a covered entity and its business associate, but the language may be adapted for purposes of a contract between a business associate and subcontractor. Where language is bracketed, it is recommended but not required under the regulations or optional depending on the services to be provided by the business associate. The sample agreement is not intended to provide legal advice or opinion. Entities should consult with legal counsel in reviewing and creating their own business associate addendums and should not adopt this BAA without first consulting with legal counsel. This BAA is drafted in light of the changes to the HIPAA rules and regulations that take effect on March 26, 2013 and is modeled after the sample document released by the Office of Civil Rights.

BUSINESS ASSOCIATE ADDENDUM

This HIPAA Business Associate Addendum (the “Addendum”) is effective as of _____, 20____ (the “Addendum Effective Date”), by and between _____ (the “Covered Entity”), and _____ (the “Business Associate”). This Addendum amends, supplements, and is made a part of that certain Agreement, dated _____, by and between Covered Entity and Business Associate as the same may be amended from time to time (the “Agreement”).

RECITALS

- A. Covered Entity and Business Associate wish to disclose certain information to each other pursuant to the terms of the Agreement, some of which may constitute Protected Health Information (“PHI”) (as defined below).
- B. Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191, applicable regulations and other guidance promulgated thereunder by the U.S. Department of Health and Human Services (“HIPAA”), and other applicable state and federal laws, including, without limitation, HITECH (as defined below).
- C. The purpose of this Addendum is to satisfy certain standards and requirements of HIPAA and the HIPAA Rules.

In consideration of the mutual promises below and the exchange of information pursuant to this Addendum, the parties agree as follows:

1. DEFINITIONS.

The following terms used in this Addendum, as well as any other terms used, but not otherwise defined, shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (“PHI”), Electronic Protected Health Information (“ePHI”), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

- a. **Business Associate** shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this Addendum, shall mean [Insert Name of Business Associate].
- b. **Covered Entity** shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this Addendum, shall mean [Insert Name of Covered Entity].

- c. Electronic Health Record shall mean any electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians or staff.
- d. HIPAA Rules shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- e. HITECH shall mean Subtitle D of the Health Information Technology for Economic and Clinical Health Act of 2009 and any regulations or other guidance promulgated thereunder.
- f. Privacy Rule shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- g. Security Rule shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

2. PERMITTED USES AND DISCLOSURES OF PHI.

- a. Business Associate may only use or disclose protected health information
 - [Option 1 – Provide a specific list of permissible purposes.]
 - [Option 2 – Reference an underlying service agreement, such as “as necessary to perform the services set forth in Agreement.”]

[In addition to other permissible purposes, the parties should specify whether Business Associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which Business Associate will de-identify the information and the permitted uses and disclosures by Business Associate of the de-identified information.]
- b. Business Associate may use or disclose protected health information as required by law.
- c. Business Associate agrees to make uses and disclosures and requests for protected health information
 - [Option 1] consistent with Covered Entity’s minimum necessary policies and procedures.
 - [Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with Covered Entity’s minimum necessary policies and procedures.]
- d. Business Associate may not use or disclose protected health information in a manner that would violate the Privacy Rule if done by Covered Entity. [Note: If the Addendum permits Business Associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add “, except for the specific uses and disclosures set forth below.”]
- e. [Optional] Business Associate may use protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
- f. [Optional] Business Associate may disclose protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- g. [Optional] Business Associate may provide data aggregation services relating to the health care operations of Covered Entity.

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.

[Note: It is highly unlikely that a Business Associate engaged only for fundraising activities would have PHI subject to Section 3 (e) or (f). You may consider permitting an introductory phrase such as “to the extent applicable” in those sections.]

Business Associate agrees to:

- a. Not use or disclose protected health information other than as permitted or required by the Addendum or as required by law;
- b. Use appropriate safeguards, and comply with the Security Rule with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Addendum;
- c. Report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement and this Addendum of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware; [The parties may wish to add additional specificity regarding the breach notification obligations of Business Associate, such as a shorter timeframe for Business Associate to report a potential breach to Covered Entity and/or whether Business Associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of Covered Entity. The regulations require Business Associate to report a breach as soon as possible but no longer than 60 days after it learned, or should have learned, about the breach. However, the longer Business Associate takes to report a breach, the less time Covered Entity has to conduct its risk assessment and take required action.]
- d. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information, provide Covered Entity with the contact information of any such subcontractors and a copy of the business associate agreements between Business Associate and such subcontractors, notify Covered Entity as soon as possible if Business Associate learns that any such subcontractor has committed a Breach, and cooperate fully in Covered Entity’s investigation of any such Breach.
- e. Make available protected health information in a designated record set to the [Choose either “Covered Entity” or “individual or the individual’s designee”] as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.524; [The parties may wish to add additional specificity regarding how Business Associate will respond to a request for access that Business Associate receives directly from the individual (such as whether and in what time and manner Business Associate is to provide the requested access or whether Business Associate will forward the individual’s request to Covered Entity to fulfill) and the timeframe for Business Associate to provide the information to Covered Entity.]
- f. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.526; [The parties may wish to add additional specificity regarding how Business Associate will respond to a request for amendment that Business Associate receives directly from the individual (such as whether and in what time and manner Business Associate is to act on the request for amendment or whether Business Associate will forward the individual’s request to Covered Entity) and the timeframe for Business Associate to incorporate any amendments to the information in the designated record set.]
- g. Maintain and make available the information required to provide an accounting of disclosures to the [Choose either “Covered Entity” or “individual”] as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.528; [The parties may wish to add additional specificity regarding how Business Associate will respond to a request for an accounting of disclosures that Business Associate receives directly from the individual (such as whether and in what time and manner Business Associate is to provide the accounting of disclosures to the individual or whether Business Associate will forward the request to Covered Entity) and the timeframe for Business Associate to provide information to Covered Entity.]

- h. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation(s); and
- i. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.
- j. Neither sell PHI nor use PHI in marketing unless requested in writing to do so by Covered Entity in writing and such sale or marketing is permitted under the HIPAA Rules. *[Note: This provision is encouraged in light of HITECH provisions.]*
- k. Retain all documentation that is required by this Addendum or the HIPAA Rules for a period of six (6) years from the date of creation or when it was last in effect, whichever is later. After the expiration of such period, Business Associate shall destroy such documentation.

4. OBLIGATIONS OF COVERED ENTITY.

- a. [Optional but encouraged] Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information. Business Associate shall strictly comply with all such restrictions.
- b. [Optional but encouraged] Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information (including a decision to opt-out from receiving fundraising solicitations), to the extent that such changes may affect Business Associate's use or disclosure of protected health information. Business Associate shall strictly comply with all such restrictions.
- c. [Optional but encouraged] Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information. Business Associate shall strictly comply with all such restrictions.
- d. [Optional but encouraged] Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if Business Associate will use or disclose protected health information for, and the Addendum includes provisions for, data aggregation or management and administration and legal responsibilities of Business Associate. A business associate agreement may, but is not required to, contain such permission.]

5. TERM AND TERMINATION.

- a. Term. The term of this Addendum shall commence as of the Addendum Effective Date, shall be coterminous with the Agreement, and shall continue in full force and effect from year-to-year, but shall terminate as of the earliest occurrence of any of the following:
 - (1) The Agreement is terminated;
 - (2) This Addendum is terminated for cause as described in Section 5(b) of this Addendum;
 - (3) The parties mutually agree to terminate this Addendum; or
 - (4) This Addendum is terminated under applicable federal, state or local law.
- b. Termination for Cause.
 - (1) Upon Covered Entity's determination of a material breach by Business Associate or by any subcontractor of Business Associate of this Addendum, Covered Entity shall notify Business Associate of its knowledge of such breach and shall have the right, but not the duty, to immediately terminate this Addendum and Agreement. Such termination shall take effect within a reasonable period of time [i.e., 30 days] after written notice from Covered Entity to Business Associate that this Addendum is being terminated, absent extraordinary circumstances, but the obligations imposed on Business Associate shall continue until the date when all PHI held by Business Associate is destroyed, returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information in accordance with Section 5, below.

In lieu of immediate termination, Covered Entity may, but does not have the duty to, provide Business Associate with an opportunity to cure the breach or end the violation within thirty (30) days.

- (2) [Optional] Upon Business Associate's determination of a material breach by Covered Entity of this Addendum, Business Associate shall notify Covered Entity of its knowledge of such breach and shall have the right, but not the duty, to immediately terminate this Addendum and the Agreement. Such termination shall take effect within a reasonable period of time after written notice from Business Associate to Covered Entity that this Addendum is being terminated, but not sooner than sixty (60) days after such written notice, absent extraordinary circumstances. In lieu of immediate termination, Business Associate may, but does not have the duty to, provide Covered Entity with an opportunity to cure the breach or end the violation within thirty (30) days.

c. Effect of Termination.

- [Option 1 – if Business Associate is to return or destroy all protected health information upon termination of the Addendum]

Upon termination of this Addendum for any reason, Business Associate shall return to Covered Entity [or, if agreed to by Covered Entity, destroy] all protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate still maintains in any form. Business Associate shall retain no copies of the protected health information.

- [Option 2—if the Addendum, authorizes Business Associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and Business Associate needs to retain protected health information for such purposes after termination of the Addendum]

Upon termination of this Addendum for any reason, Business Associate, with respect to protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the remaining protected health information that Business Associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with the Security Rule with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as Business Associate retains the protected health information;
4. Not use or disclose the protected health information retained by Business Associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Sections 2(e) and 2(f)] which applied prior to termination; and
5. Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the protected health information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

[The Addendum also could provide that Business Associate will transmit the protected health information to another business associate of Covered Entity at termination, could add terms regarding Business Associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors, could require Business Associate to certify to Covered Entity that it has either destroyed or returned all such PHI, and/or could provide for mutual decision making.]

- f. If Business Associate destroys PHI, Business Associate must destroy it only in accordance with the HIPAA Rules.
- g. Survival. The obligations of Business Associate under this Section shall survive the termination of this Addendum.

6. INDEMNIFICATION.

[Note: An indemnification provision is not required. While such provisions are generally objected to, they are typically found in BAAs and always meet with opposition.]

Business Associate shall defend, indemnify and hold harmless Covered Entity, and each of Covered Entity's affiliates, fiduciaries, officers, employees, and agents, from and against any claim or demand, damage, cause of action, liability, loss, cost, or expense, including reasonable attorneys' fees, resulting from, arising out of, or relating to, any breach by Business Associate, or any of its affiliates, directors, officers, employees, agents, subcontractors, or successors, of the terms of the Agreement or this Addendum, or any negligence or willful misconduct in the performance of its duties under the Agreement or this Addendum. Business Associate further agrees to assist and defend Covered Entity in any investigation, litigation, adjudication, arbitration, or proceeding of any kind, whether brought by the Secretary, an Individual, or any other person or entity, that may result or arise from any breach of the terms of the Agreement or this Addendum.

7. MISCELLANEOUS.

[Note: These miscellaneous provisions should be coordinated with the underlying agreement.]

- a. Regulatory References. A reference in this Addendum to a section in the HIPAA Rules means the section as in effect or as amended.
- b. Amendment; No Waiver. Upon the effective date of any federal statute amending or expanding HIPAA or any guidance, temporary, interim final or final regulations promulgated under HIPAA or under any federal statute amending or expanding HIPAA (collectively, the "HIPAA Regulations") that are applicable to this Addendum or any amendments to the HIPAA Regulations, this Addendum shall be automatically amended, such that the obligations imposed on Covered Entity and Business Associate shall remain in compliance with such requirements, unless Covered Entity notifies Business Associate otherwise. The parties agree to take such action as is necessary to expressly reflect such automatic amendments in this Addendum from time to time and to make any other amendments as is necessary for compliance with any other applicable law. Except as provided otherwise in this Section 7(b), no waiver, change, modification, or amendment of any provision of this Addendum shall be made unless it is in writing and is signed by the parties hereto. The failure of either party at any time to insist upon strict performance of any condition, promise, agreement or understanding set forth herein shall not be construed as a waiver or relinquishment of the right to insist upon strict performance of the same condition, promise, agreement or understanding at a future time.
- c. Survival. The respective rights and obligations of Business Associate under Section 3(k) (Retention of Protected Health Information), Section 5(c) (Effect of Termination) and Section 6 (Indemnification) of this Addendum shall survive the termination of the Agreement and this Addendum.
- d. No Third-Party Beneficiaries. This Addendum is between the parties hereto. Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors, any rights, remedies, obligations or liabilities whatsoever.
- e. Effect on Agreement. Except as specifically required to implement the purposes of this Addendum, or to the extent inconsistent with this Addendum, all other terms of the Agreement shall remain in force and effect.
- f. Interpretation. Any ambiguity in this Addendum shall be interpreted to permit compliance with the HIPAA Rules. The titles and headings set forth at the beginning of each Section hereof are inserted for convenience of reference only and shall in no way be construed as a part of this Addendum or as a limitation on the scope of the particular provision to which it refers. In the event of an inconsistency between the provisions of this Addendum and the mandatory terms of the HIPAA Rules, as may be expressly amended from time-to-time by the Secretary, or as a result of interpretations by the Secretary, a court, or another regulatory agency with authority over the parties, the interpretation of the Secretary, such court, or regulatory agency shall prevail.
- g. Invalid or Unenforceable Provision. The provisions of this Addendum shall be severable. The invalidity or unenforceability of any particular provision of this Addendum shall be construed, in all respects, as if such invalid or unenforceable provision had been omitted, and shall not affect the validity and enforceability of the other provisions hereof.

- h. Nonassignability: Benefits and Burdens. Business Associate may not assign its rights, or delegate its duties or obligations, under this Addendum without the prior written consent of Covered Entity, which consent shall not be unreasonably withheld. This Addendum shall be binding upon, and shall inure to the benefit of, the parties hereto and their respective successors.
- i. Governing Law. Except to the extent preempted by applicable federal law, this Addendum shall be construed, administered and governed under the laws of State of [_____].
- j. Entire Agreement. This Addendum, together with the Agreement, constitutes the entire agreement between Covered Entity and Business Associate with respect to the matters described herein. No promises, terms, conditions or obligations, other than those contained in this Addendum or the Agreement shall be valid or binding. Any prior agreements, statements, promises, negotiations, inducements, or representations, either oral or written, made by either party or agent of either party, that are not contained in this Addendum or the Agreement shall be of no force or effect.
- k. Notices. All notices hereunder shall be in writing, and either delivered by hand, or sent by mail, or delivered in such other manner as the parties may agree upon, to the following:

Covered Entity:

Business Associate:

- l. Counterparts. This Addendum may be executed in separate counterparts, none of which need contain the signatures of both parties, and each of which, when so executed, shall be deemed to be an original, and such counterparts shall together constitute and be one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have duly executed this Addendum as of the Addendum Effective Date.

COVERED ENTITY:

BUSINESS ASSOCIATE:

By: _____

By: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____

Appendix D—Clarifying Letter from HHS to AHP

**DEPARTMENT OF HEALTH & HUMAN SERVICES**

Voice - (202) 619-0403 TDD - (202) 619-3257 Fax - (202) 619-3818

[Http://www.hhs.gov/ocr/](http://www.hhs.gov/ocr/)**OFFICE OF THE SECRETARY**

Director
Office for Civil Rights
200 Independence Ave., SW Rm 506F
Washington, DC 20201

April 2, 2003

William C. McGinly, Ph.D., CAE
President, Chief Executive Officer
Association for Healthcare Philanthropy
313 Park Avenue, Suite 400
Falls Church, Virginia 22046

Dear Dr. McGinly:

Thank you for your letter to Secretary Thompson, providing the views of the Association for Healthcare Philanthropy (AHP) regarding the Department's Health Information Privacy Rule. Secretary Thompson has asked me to respond on his behalf. As you may know, the Office for Civil Rights has responsibility within the Department for implementing the Privacy Rule.

We have given careful consideration to your letter, which requests our views with respect to three issues: Patient's Department of Service Information, Business Associate Agreements, and Medical Independent Contractor Referrals, and I will comment on them in turn.

As you know, the Privacy Rule at 45 CFR 164.514(f) permits a covered entity to use protected health information without individual authorization for fundraising on its own behalf, provided that it limits the information that it uses to demographic information about the individual and the dates that it has provided services to the individual. In drafting this aspect of the Rule, the Department balanced the interest of limiting access to patients' protected health information, with the need of a covered entity to engage in fundraising. This issue was addressed in the Final Rule on December 28, 2000, and was not modified by the August 14, 2002 Rule.

As stated in the December 2000 preamble to the Rule, demographic information "will generally include, in this context, name, address and other contact information, age, gender, and insurance status. The term does not include any information about the [patients'] illness or treatment." See 65 FR 82718. Thus, your request that the Department issue guidance that would allow greater use of protected health information relating to the generic area of treatment (e.g., cancer clinic), would be inconsistent with how the Department has interpreted the term "demographic information." We will, however, take your concern into consideration as we continue to evaluate the impact of the Rule and how, in practice, it appropriately balances protection of patient privacy with the need to permit the continued delivery of quality health care.

Your letter further requests that the Department confirm that health care institutions are not required by the Privacy Rule to execute business associate contracts with their own development offices or foundations. As you point out, at 45 CFR 164.514(f)(1), the Privacy Rule states, "A

covered entity may use, or disclose to a business associate or to an institutionally related foundation..." certain protected health information for fundraising purposes. Health care institutions may use a variety of mechanisms or business arrangements for the conduct of their fundraising activities. If information is being used within a single legal entity for fundraising purposes, the Privacy Rule does not require a business associate contract. Thus, if the records management office of a hospital shares the names of patients with the hospital's development office, a business associate agreement is not needed. Of course, any such communication is limited to demographic information and dates of service. The Rule also permits patient information to be disclosed from one legal entity covered by the Privacy Rule, such as a health care institution, to a different legal entity, if the entity receiving the information is a business associate of the covered entity or an institutionally related foundation. You are, therefore, correct that the Rule permits disclosures of patient information for fundraising purposes to institutionally related foundations without a business associate agreement.

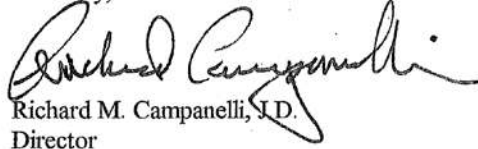
The last issue raised in your letter is whether the Privacy Rule allows a health care provider who is not a member of the covered entity's workforce (e.g., an independent contractor or a provider with staff privileges) to disclose protected health information to refer patients to the development office of the covered entity. The answer will depend on the particular facts and circumstances presented. If the provider is not a covered entity, the Rule does not restrict its use or disclosure of protected health information. Also, if the covered entity and the health care provider, who is not a member of the covered entity's workforce, participate in an organized health care arrangement (OHCA), the provider may disclose protected health information for any health care operations activities of the OHCA. See 45 CFR 164.506(c)(5). We emphasize, however, that where the purpose for sharing the information is fundraising, this is limited to demographic information and date of treatment as discussed above.

Of course, the Rule always permits disclosures of information with adequate patient authorization. An individual physician or the health care institution may use department of service information or other non-demographic information in deciding which patients to approach to ask if they would be willing to authorize the use or disclosure of their information for fundraising purposes. The authorization itself must be in writing and meet the requirements of the Rule at 45 CFR 164.508.

Thank you for sharing information about and the perspectives of AHP with us. We recognize the importance of philanthropic fundraising to the healthcare industry, and hope our response is helpful to AHP.

Please do not hesitate to contact me if you have any further questions or concerns.

Sincerely,



Richard M. Campanelli, J.D.
Director

HIPAA Checklist

Development departments and institutionally related foundations should take steps to ensure compliance with HIPAA regulations. Below is a quick checklist to get you started:

- ❑ Designate a fundraising organization “privacy officer” and assign him or her responsibility to research, develop, implement and oversee compliance for your department or foundation, and to liaison with your health care organization’s privacy officer.
- ❑ Work with your hospital or health care organization privacy officer to develop, schedule and document annual HIPAA training for your employees, volunteers, vendors and business associates about the HIPAA standards and regulations affecting their specific activities, duties and responsibilities.
- ❑ Document or review the standards for maintaining the security of patient information in your development office or foundation’s care or possession, including IT security processes and procedures (password protection, data encryption, etc.). Meet with your health care organization’s privacy officer to ensure you are in compliance with HIPAA.
- ❑ Document or review the standards and procedures for accepting, recording and complying with patient fundraising communication opt-out requests.
- ❑ Identify the individuals from your hospital or health care organization who are responsible for conducting data filtering and document the standard filters to apply to limit the use of patient information to the minimum necessary. Create policies to ensure that you and your vendors receive only permitted patient information. Discuss scenarios and establish criteria in advance to eliminate the need to make case-specific decisions regarding what and how much patient health information to use or disclose in day-to-day fundraising operations.
- ❑ Document your staff and vendors’ responsibilities and liability regarding releases of prohibited information and the procedures for handling potential breaches, and provide specific scenarios. For example, if a hospital database export accidentally provides your development office or one of your vendors with medical information beyond the permitted parameters, what is the proper procedure and timeframe for notifying the hospital privacy officer of the potential breach? What reporting or mitigation must be taken?
- ❑ Check your hospital’s business associate agreements (BAA) to ensure that all your fundraising vendors that have access to or disclose patient information, have a current HIPAA BAA and that the agreements are up to date and include the HITECH 2009 notification and liability provisions.
- ❑ Make sure everyone knows—when in doubt, apply the HIPAA Minimum Necessary rule: Is this data absolutely necessary to complete the fundraising task at hand?

