Quick Reference Guide

The Health Insurance Portability and Accountability Act

The much anticipated Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules were published January 25, 2012 to the Federal Register. The modified rules allow fundraisers expanded access to department of service, treating physician and outcome information. This is a huge gain for AHP members and the communities they serve.

- **The new rules have an effective date of March 26, 2013, with a compliance date of September 23, 2013.**
- **The information provided is updated based on the 2013 Modifications.**
- **More information can be found in the AHP publication Fundraising Under HIPAA available online (www.ahp.org) in the bookstore**

The new rules are available for download at: https://federalregister.gov/a/2013-01073.

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 in 1996 when Congress, recognizing the need for national patient privacy standards, passed the Health Insurance Portability and Accountability Act (HIPAA).

Among the many issues addressed in the legislation and subsequent regulations, specific requirements were outlined for protecting patient medical information, and civil and criminal penalties established for violations. The HIPAA Privacy Rule contains the majority of the regulations that pertain to health care fundraising.

- **Fundraising under HIPAA - The basics**
- **Regulatory history & the role of HHS**
- **Who is subject to the HIPAA Privacy Rule**
- **Important HIPAA terms & definitions**

Fundraising Under HIPAA - The Basics

NOTE: *The information provided was updated based on the 2013 Modifications to the HIPAA Privacy Rules, with an effective date of March 26, 2013 and a compliance date of September 23, 2013.*

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 did make substantial changes in the type of patient information that can be used or disclosed without patient authorization, and provides for greater patient awareness and control of their information. Below are the basics for fundraising under HIPAA.

Patient information that can be used 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

The HIPAA Privacy Rule regulations include fundraising "for benefit of the covered entity" as a "health care operation," therefore health care providers do NOT need to obtain patient authorization to use the six categories of patient health information listed above for fundraising purposes. [45 CFR § 164.501]

Patient information that requires patient authorization prior to use

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.

Notice of Privacy Practices

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 information that they may be contacted for fundraising efforts and include a statement that the patient has the right to opt out of receiving any fundraising communications.

Sample language: ***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 INSTITUTION] 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 INSTITUTION].

Fundraising opt out

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 (including telephone solicitations). The opt-out must:

- Be a clear and conspicuous part of the materials sent 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.

Sample language: ***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 mail In the alternative, you can call our telephone number [either the local numbers [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.***

Business Associate Agreements (BAA)

HIPAA recognizes that a heath care provider may have relationships with other entitites and vendors that perform services on their behalf, and outlines requirements to ensure the protection of patient information through the use of business associate agreements.

A hospital or health care organization must have a business associate agreement with a fundraising vendor if patient information will be shared or used by the vendor. Such agreements ensure that vendors are aware of their responsibilities in protecting patient information, the breach notification processes, and their liability in the case of HIPAA violations.

Covered entities must ensure that they obtain satisfactory assurances required by the Rules from their business associates, 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 it must ensure that the subcontractor has systems in place to comply with applicable portions of HIPAA and will protect any PHI it receives. A sample BAA is available online at HHS' website for HIPAA: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

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.

Regulatory History & HHS Role

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.

Regulatory history:

- January 2013 - HHS publishes its long-awaited Modifications to the HIPAA Privacy Rule in the Federal Register on January 25. The modifications offer clarity to the Final Rules that impact the Opt Out provision and the Notice of Privacy Practices, as well as make changes that allow fundraisers a better way to communicate with patients.

- July 2010 - HHS announces proposed rule changes to the HIPAA Privacy, Security, Enforcement and Breach rules, including changes to the fundraising section of the Privacy Rule.

- October 2009 - HHS issues Interim Final rule changes to the Enforcement Rule, which allows the HHS Secretary to impose civil monetary penalties for violations and significantly increases the penalties for HIPAA violations.

- August 2009 - HHS issues an Interim Final Breach Notification Rule based on section 13402 of HITECH, requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

- February 2009 - The Health Information Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act of 2009 (ARRA), is enacted, making a number of changes to the HIPAA Privacy, Security and Enforcement Rules. HHS is mandated to issue regulatory guidance related to these changes.

- February 2006 - HHS issues the Final Enforcement Rule.

- April 2003 - HHS issues the Interim Final Enforcement Rule.

- February 2003 - HHS issues the Security Rule.

- August 2002 - HHS releases modifications to the Privacy Rule.

- December 2000 - HHS publishes the Privacy Rule after considering more than 52,000 comments.

- November 1999 - HHS releases proposed privacy regulations governing individually identifiable health information for comment.

- August 1996 - The Health Insurance Portability and Privacy Act (HIPAA) is enacted. HHS is designated the authority for developing the rules and standards in support of the legislation, including the electronic exchange, privacy and security of health information.

Who is Subject to HIPAA

NOTE: *The information provided was updated based on the 2013 Modifications to the HIPAA Privacy Rules, with an effective date of March 26, 2013 and a compliance date of September 23, 2013.*

.

HIPAA uses the term “covered entities” to describe those organizations that are subject to HIPAA and the Privacy Rule. A covered entity is a:

- **Health care provider** (hospital, clinic, doctor, dentist, nursing home, home health care provider),
- **Health care clearinghouse** (including billing services), or a
- **Health plan,** that transmits certain types of health information in electronic form.

A hospital or health care organization fundraising department or institutionally related foundation must adhere with HIPAA regulations, although the responsibility for compliance, and addressing breaches or violations, resides with the health care provider.

Covered entities are required to assign a Privacy Officer that develops, implements and oversees the organization's compliance with the HIPAA Privacy Rule.

A development department or related foundation should work closely with their Privacy Officer in training staff, board members and volunteers, and in developing HIPAA compliant processes and procedures for the fundraising organization.

Important HIPAA Terms & Definitions

NOTE: *The information provided was updated based on the 2013 Modifications to the HIPAA Privacy Rules, with an effective date of March 26, 2013 and a compliance date of September 23, 2013.*

The following are key terms and concepts that apply to fundraising under HIPAA and the Privacy Rule.

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; 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. The rule also allows the use of a patient's insurance status, although in the rule it does not constitute demographic information. HIPAA permits such non-medical identifying information to be used for fundraising efforts without patient authorization.

The HIPAA Privacy Rule regulations include fundraising "for benefit of the covered entity" as a "health care operation," therefore health care providers do NOT need to obtain patient authorization to use demographic information for fundraising purposes. [45 CFR § 164.501]

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.

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 communications (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.

HIPAA regulations state that a "covered entity must include in any fundraising materials it makes to an individual under this paragraph [a patient] a description of how the individual may opt out of receiving any further fundraising communications." [45 CFR § 164.514(f)(2)]

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.

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.