The HIPAA Effect:

Considerations for Fundraising After the Health Insurance Portability and Accountability Act

A paper about the basics of HIPAA
and what you need to consider
as you build your online database.

July 2008

Brought to you by:

Changing Our World, Inc.
FUNDRAISING PHILANTHROPY

convio®

INTRODUCTION

Eight years after Congress passed the Health Insurance Portability and Accountability Act (HIPAA), professionals working in healthcare philanthropy have discovered that HIPAA was not the end of fundraising as we knew it. Initially, when HIPAA was enacted in 2000, there was great fear and uncertainty among healthcare providers and development officers. Reactions across the nation and among healthcare organizations varied widely: some predicted the end of healthcare fundraising, whereas other more rational people viewed it as a manageable challenge.

HIPAA has proven to be another step in a society that becomes more complex and more stringently regulated every year. Healthcare providers and medical foundations have noted that from a development/fundraising perspective, HIPAA has little effect on fundraising — yet it remains a concern to fundraisers, online and offline.

This paper covers the basics of HIPAA and what you need to consider about your constituents as you build your online database.

A BRIEF HISTORY OF HIPAA

Each time a patient sees a doctor, is admitted to a hospital, fills a prescription, or sends a claim to a health plan, a record of their confidential health information is made. In the past, family doctors and other healthcare providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the protection of patients' privacy and confidentiality.

Congress recognized the need for national patient record privacy standards when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The law required new safeguards to protect the security and confidentiality of that information. At the same time, the law gave Congress until August 21, 1999 to pass comprehensive health privacy legislation. When Congress did not enact such legislation prior to the deadline, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

In November 1999, HHS published its proposed regulations to guarantee patients' new rights and protection against the misuse or disclosure of their health records. During an extended comment period, HHS received more than 52,000 communications from the public. In December 2000, HHS issued a final rule that made significant changes in order to address issues raised by the public's feedback. The HHS Secretary opened the final rule for comment to ensure that it would protect patients' privacy without creating unanticipated consequences that might harm patients' access to or quality of care. After that comment period, the President and HHS Secretary decided to allow the rule to take effect on April 14, 2001, as scheduled, and to make appropriate changes in the next year to clarify the requirements and correct potential problems that could threaten access to or quality of care.

There are three parts to HIPAA: Privacy, Code Sets, and Security. In addition, Security is broken down into four parts: Administrative Procedures, Physical Safeguards, Technical Security Services (which covers "data at rest," within the local area network), and Technical Security Mechanisms (which covers "data in transmission," over any type of communications network).

HIPAA applies to "covered entities." A covered entity is a healthcare provider, a healthcare clearinghouse and a health plan. For our purposes, "health plans" are defined to include insurance companies that issue, among other types of health insurance, long term care insurance.

HIPAA-compliant authorization is one that has each of the following elements:

- A specific description of the information to be disclosed (e.g., "any personal health information, records or data concerning my past, present or future mental, physical or behavioral health or condition")
- A specific description of the person(s) or class of persons to whom the information is to be disclosed
- A specific description of the person(s) or class of persons who is authorized to disclose the information (e.g., "any physician or other medical practitioner, any hospital, clinic, or other health-related facility, any medical testing laboratory or fundraiser/development office/foundation")
- A description of the purpose of the authorization
- An expiration date or event
- A signature and date
- A statement detailing the right to revoke the authorization, and instructions how to revoke it
- A statement that if the person does not sign the authorization, the purpose of the authorization may not be able to be met
- A statement that the information being disclosed is subject to re-disclosure and may no longer be protected by federal privacy regulations

Under HIPAA, healthcare organizations must obtain written permission from individuals — by way of a signed authorization form — before they use or share health-related information for marketing and certain other purposes. An authorization form documents the patient's permission to allow use or disclosure of their protected health information *for purposes other than treatment, payment, or healthcare operations.*

Healthcare operations include **(but are not limited to)**:

- Certain fundraising activities for the covered entities' own benefit
- Quality assessment and improvement activities
- Business planning, development and management activities
- Evaluating healthcare professionals and plans
- Training healthcare professionals

Healthcare organizations may not withhold treatment, enrollment in a health plan, benefits eligibility, or payment as a means of obtaining patient authorization. Authorization forms are a specific and comprehensive type of written permission that should be written in plain language.

HAS HIPAA AFFECTED FUNDRAISING?

AHP Request for Clarification: The Privacy Rule recognizes that philanthropic fundraising is a part of healthcare operations. However, the final rule limits protected healthcare information to be used or disclosed for fundraising to demographic information and the date of treatment. The Association for Healthcare Philanthropy (AHP) believes that the Privacy Rule would be strengthened by allowing development office employees of not-for-profit hospitals and their institutionally related foundations to have access to one additional piece of information that in the healthcare world is essentially demographic in nature: their patients' department of service (PDS).

HHS Response: The Department of Health and Human Services (HHS) gave a detailed response to our question. The short answer: HHS will continue to work with AHP on this issue.

> *"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."*

Fundraiser Response: The president of a medical center on the west coast believes the HIPAA/fundraising issue has not been an issue for his department:

> *"Each day we receive a list of patients who are in the hospital. It does not include information that would violate HIPAA information, such as medical information, who their doctor is, etc. We do make contact from that list with patients who already have a relationship with the Foundation, and we use information from this list to send appeal letters for our Annual Fund. Once the information is gleaned, the listed are destroyed.*
>
> *In reality, the HIPAA guidelines have not been much of a hindrance."*

A unique response was received from the president of a truly "arms length" foundation, one that is not part of the health system it supports:

> *"As you know, we are not part of the hospital healthcare system in any way except that we share some of the same name. As an independent not-for-profit organization (I think we are one of only two in the US), we cannot access or even have a business associate agreement for patients' information.*
>
> *The legal and ethical way in which we are able to have any patient names at all is by the following:*
>
> *Request that the hospital IT department create a list of patients based upon specific demographics, age, private pay, no Medicaid, no prisoners, no mental health, no minors, etc. Once this information has been compiled, a CD is created and sent to a third party.*
>
> *A letter is created for the hospital CEO to sign.*
>
> *A response card is created allowing the letter recipient to respond directly to the Foundation, or be removed from any mailing list. If the patient decides to respond with the response card with which a business reply envelope is provided directly to the Foundation, our legal counsel has deemed that the patient has given permission to the Foundation for further contact.*
>
> *The third party (mail house) develops and prints the letter, the response card, and both envelopes. Once this is done, the third party destroys the CD so no one has any information nor has seen any of the names, etc.*
>
> *We do this every six months. We actually have been successful in getting new prospects, as well as donors. Not a great deal of money, but at least the opportunity to voice an opinion about their care that is shared with the hospital so they can either feel proud or take corrective actions."*

Specific disease-related fundraising continues to challenge many healthcare providers that service a non-disease specific patient base. There are several creative ways that healthcare institutions tackle this challenge and remain HIPAA compliant. One of the simplest ways of garnering disease specific information is to include on the initial and all subsequent foundation or development department mailings an opportunity for the recipient to support or seek additional information on a specific disease or diseases. Additionally, it can be extremely helpful if modest brochures (e.g., 3 fold 8 1/2 x11, response cards, self-mailers) are placed in patient and family waiting areas. The marketing piece should tie the support of a specific disease to new equipment, research, patient comfort, education or some other philanthropic challenge. Patient testimonials and successful outcomes are particularly noteworthy and helpful for fundraising.

HIPAA AND YOUR DONORS

Follow the letter of the law, use wisely the information you can get, be creative in your communications, demonstrate how philanthropy makes a difference, and deliver your message in very personal, human and community terms. Also keep in mind that one of the most onerous aspects of HIPAA compliance is the problem of computer and paper archives. Archives of most foundation and hospital development offices contain some amount of patient information because they were created before HIPAA was a concern. Hospital risk managers may be averse to allowing fundraisers to keep and access old files that contain patient information. Privacy officers may wish to segregate files created before and after April 14, 2003, and limit access to the older files that contain identifiable patient health information.

Unless a patient signs a special authorization, the HIPAA Privacy Rule will limit fundraisers' access to a patient's name, address, age, gender, insurance status, and the date the individual was treated. Many analysts interpret the Privacy Rule to mean that fundraisers cannot access information about the doctor or practice area where a patient was treated. Additionally, under HIPAA, donor prospects must be given the opportunity to opt out of fundraising activities, a requirement that pushes new tracking and record-keeping responsibilities upon healthcare fundraisers.

Many fundraisers are looking to a signed authorization from a patient to lessen the impact of this regulation. The authorization needed to sidestep some Privacy Rule restrictions must include a list of components, including the duration and specific purpose of the authorization. It seems unlikely that any foundation or development office would be able to cover its entire prospect pool with signed authorizations in order to minimize the operational impact of HIPAA.

HIPAA AND ONLINE PHILANTHROPY

Organizations can manage their online data in the same way that they manage the data contained in their offline databases. Avoiding detailed medical information is the safest method to gathering information from online constituents. Segmentation and imports from offline databases can raise specific issues for organizations that want to collect former patient information to target fundraising messages. Soliciting patient information can be managed within HIPAA's regulations by following several guidelines:

- **Link Your Databases:** Always link your online database with your offline fundraising database, never to any patient record databases. Large hospitals often give their foundations or fundraisers simple biographical information for their fundraising databases. This information is enough to start a fundraising or communication dialogue with your constituent. Avoid asking for specific medical details in your online registration forms (e.g., doctor information, specific medical conditions, or details about medical history).

- **Stay General:** General questions can still provide valuable segmentation information for targeted messaging. Ask for general information with your online constituent biography forms (e.g., "Does heart disease run in your family?", "When did you stay with us?", "Is your family covered by medical insurance?").

- **Make It Optional:** Constituent details should never be mandatory fields on your online forms. Allow constituent to choose whether they want to provide specific information. Name, email, and zip code can be mandatory fields, but avoid forcing constituents to provide other details.

- **Begin with a Positive Welcome:** Place every former patient into a welcome email series, which consists of two or three individual emails that are sent six to eight weeks following treatment. Stay transparent and invoke warm messaging to help the patient understand how they can help the hospital. Avoid fear tactics, statistics about healthcare related to the patient's condition, or any negative messaging. Patient and hospital success stories are one example of positive messaging. Success invites response.

- **Solicit Success Stories:** Patient success stories provide heartwarming content. Always solicit stories directly and obtain a signed waiver for the information, which should include a description of how and where the information will be used. Never use patient photographs from specific procedures and always try to photograph patients professionally or use photos following their stay. Stories should never mention specific treatments or detailed information about a patient's illness.

- **Message Boards and Social Networks:** Message boards and social networks can provide potentially hazardous sources of communication with constituents through user-generated content that is not pre-screened. When patients share medical information under your hospital's online auspices, this could be interpreted as a HIPAA violation by some constituents. Legal disclaimers and warnings should be provided as a separate callout with a prominent, or even mandatory, page that must be accepted before constituents participate in a discussion. Be sure that patients do not share doctor names or specific treatment information related to their illness and that the hospital will not solicit this information at anytime. Your communication staff should be prepared to moderate discussions or posts to avoid any issues which arise.

In short, while HIPAA remains a concern to fundraisers - online and offline – a basic but strong understanding of the rules will protect your healthcare organization, while allowing successful fundraising to continue.

- Commonly Asked Questions About HIPAA from the AHP
  http://www.ahp.org/government-relations/hipaa/faq-on-hipaa.php

- HHS HIPAA Standards
  http://www.hhs.gov/ocr/hipaa/

- Centers for Medicare & Medicaid Services HIPAA Overview
  http://www.cms.hhs.gov/hipaaGenInfo/

Changing Our World is one of the leading philanthropic services companies in the world, providing tailored solutions to non-profits and philanthropists. With headquarters in New York and offices in London, Los Angeles, Washington, DC, and Boston, Changing Our World raises tens of millions of dollars annually for nonprofit clients, and assists corporations, foundations, and individuals in achieving their goals in philanthropy. Our services include fundraising, corporate philanthropy, private philanthropy, strategic planning, ephilanthropy, and information resources.

For more information, please visit **www.changingourworld.com**.

Convio is a leading provider of on-demand constituent relationship management software and services to nonprofit organizations to enable nonprofit organizations to more effectively raise funds, influence public policy and support their missions by leveraging the Internet to build strong relationships with constituents. The company's online constituent relationship management, or eCRM, solution includes a suite of on-demand software modules for fundraising, advocacy, email marketing and Web content management complemented by a portfolio of best-in-class consulting services.

For more information, please visit **www.convio.com**.

This document is solely intended for information regarding the Health Insurance Portability and Accountability Act (HIPAA) and does not constitute as, or substitute for, any legal counsel or legal advice from a licensed attorney.