HIPAA UPDATE

October 2, 2002

FUNDRAISING Post-HIPAA

The final federal privacy regulation (the "Privacy Rule") promulgated by the Department of Health and Human Services ("HHS") pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") considerably limits the ability of covered entities to use and disclose protected health information in their fundraising activities. The August 14 modifications did not affect the fundraising limitations. This advisory summarizes the fundraising requirements of the HIPAA Privacy Rule and discusses some areas of confusion that have resulted from these requirements.

Fundraising Requirements

First, a covered entity can obtain authorization of the individual using the form prescribed by HIPAA to use patient information - including demographic information as well as information about the patient's health condition - for fundraising activities. However, the Privacy Rule prohibits one from conditioning the availability of treatment on signing such an authorization. Accordingly, existing practices of obtaining a signed consent for fundraising activities at the time one obtains consent to treatment will need to be modified in two ways: (1) The form of the fundraising authorization will need to meet the HIPAA format requirements, and (2) It will need to be examined carefully to ensure that the form-signing process during the patient admissions process does not lead the consumer to believe that the fundraising authorization must be signed in order for treatment to be available.

Second, in the absence of an explicit individual authorization, the Privacy Rule states that a covered entity may use or disclose patient information for its fundraising activities only if *each* of the following conditions (if applicable) are met:

(1) Only demographic information and the dates an individual received health care can be *used* in fundraising—not disease related information. ("Demographic information" includes a patient's name, address, other contact information, age, gender, and insurance status.)

(2) A covered entity may *disclose* the information in item 1 for fundraising purposes, but only to (a) the covered entity's business associate, pursuant to a business associate agreement; or (b) an institutionally-related foundation. (An "institutionally related foundation" is a nonprofit charitable foundation qualified under section 501(c)(3) of the Internal Revenue Code that has "an explicit linkage to the covered entity" in the foundation's charter statement of charitable purposes.)

(3) The covered entity's notice of privacy practices must state that the covered entity may use and disclose protected health information for fundraising purposes.

(4) Any fundraising materials must include a description of how the individual may opt-out of receiving any further fundraising communications.

(5) Covered entities must make reasonable efforts to ensure that individuals who opt-out are not sent subsequent fundraising communications.

Significant Issues for Current Fundraising Practices

The majority of the fundraising issues arise in connection with requirements one and two, and in dealing with the implications of corporate and HIPAA compliance structure decisions.

Issue 1. Relationships with Charitable Organizations. In the preamble to the Privacy Rule, HHS states that an organization with a "general charitable purpose, such as to support research about or to provide treatment for certain diseases, that may give money to a covered entity" is *not* an institutionally related foundation "because its charitable purpose is not specific to the covered entity." Disclosures to such an entity for fundraising thus would require patient authorization.

(2) Related Not-For-Profit Entities. The covered entity's patient information may be used to raise funds only for the benefit of the covered entity, and *not* related entities that may be served, for example, by the same institutionally related foundation. For example, a hospital will not be able to raise funds for a sister corporation that is a skilled nursing facility; a university would be precluded from using its hospital's information to raise funds for research in a related area by its academic department; a religious group or charity-owned hospital would be precluded from using patient information in combined fundraising efforts—for example, to benefit a feeding program for children, a children's hospital, an immunization outreach program, a foster-care program, and a school.

(3) Targeted Mailings. A covered entity may not target fundraising based on any criteria such as treatment received, health status, or unit of the hospital where care was rendered. Targeted mailings to new parents, cancer patients, or neurology patients, for example, as part of a capital campaign for a specific project area would be an impermissible use of protected health information.

(4) Filtering Databases. "Filtering" data based on any criterion derived from protected health information is prohibited, without individual authorization. For example, a covered entity may not run a query of its patient database to create a list of patients with certain diagnoses—or to eliminate patients with certain diagnoses from general fundraising mailings—because such query would be considered an impermissible use of diagnosis information for fundraising purposes. A covered entity may, however, attempt to identify patients that are more capable of donating by comparing its patient list against publicly available or purchasable wealth databases, because the wealth database is not protected health information. The resulting list of patients' demographic information and treatment dates may be used and disclosed for fundraising as discussed above.

(5) Existing Fundraising Databases. Databases held by the covered entity after April 14, 2003 will be governed by the privacy rule, even if they were compiled before that date. However, if a covered entity's fundraising activities are conducted by a *separate legal entity* that is not a covered entity, the databases of the separate fundraising entity that were created prior to the compliance date will not be subject to the requirements of the Privacy Rule, even if they contain more than demographic information and dates of service at the covered entity. After the compliance date, however, further disclosures of information from the covered entity to its fundraising entity must meet the requirements of the Privacy Rule.

(6) A Corporate Entity Catch-22. If a covered entity's fundraising activities are conducted through a division or component of the covered entity rather than a separate legal

entity, the "hybrid entity" provisions likely cannot be used to protect existing databases from the new fundraising limitations, because fundraising activities are defined as "health care operations." Under the hybrid entity provisions, covered functions and business associate-type activities must be included within a covered entity's health care component, subjecting them to the rule's fundraising limitations.

(7) Fundraising Communications. As of April 14, 2003, all fundraising communications by or on behalf of the covered entity must meet the HIPAA requirement for opt-out and inclusion of fundraising in the covered entity's HIPAA notice. This is true even if the mailing list used in the fundraising communication was compiled before the compliance date. Technically, the HIPAA requirements for notice and consumer opt-out are not violated when a third party or an institutionally related foundation raises funds on behalf of the covered entity using contact information in commercial databases not compiled from patient information. However, consumers who receive a mailing from or on behalf of a covered entity do not know that their name was obtained from some non-protected source. Accordingly, on consumer protection grounds alone, it seems likely that the HIPAA notice and opt-out standard for fundraising will become the norm in health care fundraising, no matter the source for the mailing list.

* * * *

If you have questions,
please do not hesitate to contact
Donna Boswell, Melissa Levine, or Marcy Wilder
(202) 637-5600.