



Connecting People • Enriching Lives

313 Park Avenue, Suite 400
Falls Church, VA 22046
www.ahp.org

March 5, 2009

The American Recovery and Reinvestment Act of 2009 - What Health Care Fundraisers Need to Know

Health Care Sector Funding

The American Recovery and Reinvestment Act of 2009 allocated 150 billion dollars to the U.S. health care sector. Congress distributed these funds to a variety of health subsets, including \$1.1 billion for comparative effectiveness research, \$1.4 billion for the construction and renovation of health care facilities, \$19.2 billion for the improvement and advancement of health care technology, \$2 billion for construction and the improvement of services and health care technology at community health centers, \$338 million for Medicare payments to teaching hospitals, hospices, and long-term care facilities, and \$50 million to DHHS for the improvement of security in health care technology. Most of these funds will be spent within two years.

Changes to HIPAA Privacy and Security Provisions

The American Recovery and Reinvestment Act of 2009 (H.R.1) also made substantive changes to the HIPAA privacy and security regulations. While none of the changes has any significant impact on health care fundraising, development offices should be aware of the revisions and the implications.

Business Associates

The original HIPAA regulations refer to and provide requirements for “business associates” ([See AHP HIPAA Special Analysis, Question 4](#)) that have access to patient information. An institutionally related foundation is considered part of “health care operations,” and is not considered a business associate. Therefore, a business associate agreement with the health care provider is not required. However, if a fundraising entity (a consultant, firm or fundraising services provider) that is not part of the health care provider or its institutionally related foundation, will have access to any patient information, they must enter into a business associate contract with the health care provider that meets regulatory standards. These provisions of HIPAA have not changed. What *has* changed is accountability and liability

New provision regarding direct liability

Business associates are now directly accountable to Federal and State authorities for compliance with HIPAA privacy and security rules.

Business associates previously may have been liable to the health care provider (covered entity) with which they contracted, for any violations of the contract. However, they could not be directly subject to the penalties and provisions imposed by HIPAA if found in violation of privacy regulations. H.R.1 changes this—the potential liability of a business associate under contract with a health care provider is now substantially increased, as they are now subject to HIPAA penalties as enforced on the federal and state levels.

Breach responsibility

H.R.1 imposes new responsibilities for both the health care provider and business associate that discover a privacy breach (as defined in H.R.1 section 13400). Both are now responsible for reporting breaches within 60 days. Also, the HHS Secretary now has an obligation to submit an annual report to Congress with all breach information.

H.R.1 also clarifies *exceptions* to what is considered a breach, including the unauthorized release of patient information, where the unintentional access or use was as part of a professional relationship and the information is not used or disclosed further.

Opt-Out Requirement Defined

H.R.1 does not change the use of limited protected health information for fundraising activities under HIPAA. A covered entity may continue to use the same limited information as was previously permitted.[\[See AHP HIPAA Special Analysis, Question 1\]](#) The health care organization's notice of privacy practices still must contain the same reference to the use of PHI for fundraising purposes as previously required. The health care organization or foundation acting on its behalf must, as before, include an opt-out provision in any fundraising materials.[\[See AHP HIPAA Special Analysis, Question 2\]](#) H.R.1 does, however, clarify that patients must be offered a clear and conspicuous opt-out for written fundraising communication.

The only change H.R.1 makes in this area is that the HHS Secretary has been directed to adopt a rule, which provides that “any written fundraising communication that is a health care operation...shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communications to elect not to receive any further such communication.” This does not change the existing opt-out requirement, but simply directs the Secretary to define what constitutes appropriate opt-out language.

H.R.1 further states that “when an individual elects not to receive any further such communication, such election shall be treated as a revocation of authorization...” Since the release of information for fundraising does not require authorization, this language does not effectuate a significant change. However, this language does change one aspect of the prior opt-out language, which stated that any revocation must be received in writing. The new provision in H.R.1 does not specify that an opt out request must be in writing.

Changes to HIPAA Enforcement

H.R.1 does substantially change the enforcement of HIPAA violations. As noted above, business associate are now directly accountable to authorities for compliance with HIPAA privacy and security rules. The HHS Secretary is now *required* to impose penalties in cases of willful neglect. There has been an increase in civil monetary penalties, up to \$1.5 million, for repetitions in one calendar year, and State Attorney Generals are now authorized to take civil action. In addition, the HSS Secretary is now required to conduct periodic audits. Also, vendors that handle personal health records, but are not HIPAA covered entities, will fall under the jurisdiction of the FTC regarding breaches of patient information.

Studies, Reports & Other Actions Required by H.R.1

- A study must be conducted by HHS and FTC to be presented to Congress on privacy and security issues regarding personal health records.
- The Office of Civil Rights must create an education initiative on the use of personal health care information and patients' rights under HIPAA.
- Privacy Officers will be designated in each HHS region.
- HHS will produce an annual report on enforcement.
- HHS will produce a study on implementation of the de-identification requirements.

What does this mean for you?

- All health care organizations (covered entities) should examine their business associate agreements to determine in they are in compliance with the new requirements.
- Foundations should review their operations to ensure that they are in full compliance with the existing and new security and privacy requirements of HIPAA. Any vendors or consultants who will be accessing patient information should have a business associate agreement in place with the health care organization that reflects the new requirements outlined in H.R.1.
- Foundations and development offices should be prepared to handle non-written opt-out requests.
- Foundations and development office should be prepared to comply with the HHS Secretary's ruling defining what constitutes appropriate opt-out language.