

February 2003

## **FUND RAISING UNDER HIPAA — THE PRIVACY RULE SPECIAL ANALYSIS**

FROM

STUART R. SMITH, FAHP – CHAIR

WILLIAM C. MCGINLY, PH.D., CAE – PRESIDENT, CHIEF EXECUTIVE OFFICER

Reviewed and Presented by AHP Legal Counsel – Peter Parvis, Esq.: Venable,  
Washington, DC

### **Background**

In 1996, Congress recognized the need for national patient privacy standards and, as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), set a three-year deadline for it to enact such protections. HIPAA also required that, if Congress did not meet this deadline, the Department of Health and Human Services (HHS) was to adopt health information privacy protections via regulation based upon certain specific parameters included in HIPAA. Congress did not enact health privacy legislation.

HHS proposed federal privacy standards in 1999 and, after reviewing and considering more than 52,000 public comments on them, published final standards in December 2000 (the “2000 Final Rule”). In March 2001, HHS Secretary Thompson requested additional public input and received more than 11,000 comments, which helped to shape the improvements proposed in March 2002. On August 9, 2002, HHS Secretary Thompson issued the comprehensive federal regulation. The final Privacy Rule was published in the Federal Register on August 14, 2002 (the “2002 Final Rule”) and it takes effect April 14, 2003. The privacy rule is part of a set of standards required under HIPAA’s “administrative simplification” provisions. The privacy rule is available online at <http://www.hhs.gov/ocr/hipaa/>.

Most covered entities have until April 14, 2003, to comply with the patient privacy rule; under the law, certain small health plans have until April 14, 2004 to comply.

### **Requirements for Fund Raising**

For purposes of fund raising, the health provider (called a “covered entity” under the Privacy Rule) must comply with these new regulations effective on April 14, 2003. Consequently, current professional fund-raising practices, as these practices are conducted by Association for Healthcare Philanthropy (AHP) members today, may continue until the implementation date without modification.<sup>1</sup>

---

<sup>1</sup> This analysis is not intended to provide legal advice, and does not discuss state law or other federal law that may have an impact on individual situations. State law may currently impose limitations, which will remain in effect, and more restrictive state laws are not pre-empted even when these regulations go into effect.

AHP successfully educated HHS in 2001 to continue to allow covered entities access to demographic patient information for fund-raising purposes while denying complete access to patient medical records. Only *demographic information* may be used in fund-raising efforts with the restrictions contained in the regulations and detailed in the analysis which follows. For the first time in health care's history, even though the Association for Healthcare Philanthropy members are part of "health care provider operations," we no longer have access to medical record information.<sup>2</sup>

Part of AHP's education effort with HHS demonstrated that our members were interested in protecting their obligation and right as not-for-profit health care providers to conduct fund raising in order to benefit the community. We noted that AHP's interest was in maintaining access to limited information about grateful patients and families. The HHS favored AHP's position and reversed its original statement in the proposed regulations, which would have denied us access to medical records *and* demographic information. This was a major success for AHP and philanthropy in health care as philanthropy relates to not-for-profit health providers and institutionally related foundations. AHP is grateful for the understanding and positive action HHS issued in its final regulations.

Still, there are specific requirements we must now meet, and a major educational undertaking we must launch to inform our donors, trustees, CEOs and administrators (compliance officers and legal counsel), and the public to correct confusion and bring clarity to the issue of how professional not-for-profit health care fund raisers employed by the provider, can and should act. Our obligation is to promote philanthropy in order to become more effective in providing for community needs and becoming recognized as the health care resource to the community and those we serve.

To that end, the Association for Healthcare Philanthropy posed five important questions concerning the Privacy Rule and requested that AHP's legal counsel (Peter Parvis, Esq. at the firm of Venable, Washington, D.C.) provide advice to assist us in complying with the privacy regulations as they pertain to our philanthropic efforts and responsibilities. We suggest you use the analysis and conclusions sections which follow with your donors, trustees, CEOs, administrators, and the public as we move into the implementation phase of these regulations.

The **Questions Presented and Conclusions** (the "short answer") section is intended to address the most common issues raised concerning the privacy regulations regarding fund raising. The more detailed **Discussion** (the "long answer") section is intended to give you an in depth understanding of the issues and implementation of the regulations. A **Definitions** section and a sample business associate agreement (provided by HHS) are included at the end of the analysis. Finally, as you begin your review, please do not hesitate to contact AHP with any specific questions you may have.

---

<sup>2</sup> Once again, state privacy and confidentiality statutes limit the release of patient records in most states and other federal law places explicit limits on certain types of medical information – most notably in the area of HIV, substance abuse, behavioral medicine, and abortion. This analysis only discusses the impact of the new HIPAA regulations.

## — Question 1 — Authorization, Notice of Privacy Practices

**Is the health care provider required to obtain authorization of former and current patients prior to sending them fund-raising materials?**

### Short Answer

*Response/Conclusion:*

Authorization is **not required** when the fund-raising entity is using **only the demographic piece** of the protected health information (PHI) or the dates of service. According to the regulations, permissible PHI does not require authorization for fund-raising purposes. The patient's authorization is required to use any PHI other than dates of service or demographic information in fund raising (See Question 3). Of course, a fund-raising initiative that does not require the use of PHI (i.e., using a mailing list that is obtained without use of any patient data) does not raise HIPAA issues.

HHS states that “[d]emographic information<sup>3</sup> is not defined in the rule, but will generally include [for the purpose of fund raising] name, address and other contact information, age, gender, and insurance status.” *Preamble 45 CFR § 164.514(f)*. In the following exchange, HHS further clarifies the meaning of “demographic information” and the use of non-demographic information in fund raising:

*Comment:* Several commentators asked us to address the content of fund-raising letters. They pointed out that disease or condition-specific letters requesting contributions, if opened by the wrong person, could reveal personal information about the intended recipient.

*Response:* We agree that such communications raise privacy concerns. In the final rule, we limit the information that can be used or disclosed for fund raising, and **exclude information about diagnosis, nature of services, or treatment**. *Id.* (emphasis added).<sup>4</sup>

*a. Permissible Information<sup>5</sup>* Note: There is no regulatory source for this advice, other than the Preamble to the 2000 Final Rule.

---

<sup>3</sup> We note that the dictionary definition of “demographic” would not support HHS’ statement in the Preamble, but an administrative agency’s contemporaneous pronouncement of what it intended its regulations to mean is generally afforded substantial weight. The statement in the Preamble is the only definition available.

<sup>4</sup> Of course, such information could be used with the patient’s authorization. This Memo assumes that authorization will not be sought in the great majority of cases. We note again that this list of impermissible items is found only in the Preamble, and is not found in the regulation itself.

<sup>5</sup> The Privacy Rule was proposed in 1999 and initially adopted as a final rule in December 2000 at 65 Fed. Reg. 82461-82829 (12-28-2000) (“the 2000 Final Rule”). Substantial amendments were proposed in March, 2002, and an amended final Privacy Rule was adopted in August 2002 (the “2002 Final Rule”). The fund-raising provisions were not amended in the 2002 Final Rule, and there is no discussion of the fund-raising issue in the Preamble to the 2002 Final Rule. Therefore, guidance on fund raising is found primarily in the Preamble to the 2000 Final Rule, pertinent parts of which are appended to this document.

Protected health information that can be utilized for fund-raising purposes without obtaining a patient's authorization includes:

- Date of Service [45 CFR § 164.514(f)(1)]
- Demographic Information 45 CFR § 164.514(f)(1) [all of the above are discussed as “demographic information” in the Preamble to the 2000 Final Rule]
- Name
- Address
- Other contact information (phone numbers, e-mail, etc.)
- Age
- Gender
- Insurance status

*b. Impermissible Use and Disclosure*

PHI that cannot be used without a patient first signing an authorization includes:

- Diagnosis
- Nature of services
- Treatment
- Place within health care provider where patient receives treatment that identifies the treatment, such as:
  - Department of Psychiatry
  - Department of Obstetrics
  - Department of Radiation Oncology

**The Notice of Privacy Practices** (Notice) is the primary privacy tool. A health care provider that intends to use protected health information to contact a patient to raise funds, must give the patient a “Notice of Privacy Practices”, which contains a separate statement that “[t]he covered entity may contact the individual to raise funds for the covered entity...” 45 CFR § 164.520(b)(1)(iii). From and after April 14, 2003, health care providers or other covered entities with direct patient contact must use a good faith effort to obtain a signed **Acknowledgment** of receipt of the Notice from patients at the time of the first encounter with the patient.

Additionally, grateful patients who are listed on a provider's donor database prior to the compliance date need not receive individual copies of the Notice of Privacy Practices until their next encounter with the provider as a patient. At such time, the Notice of Privacy Practices must be a part of the admissions process.

You must include a fund-raising sentence in the Notice of Privacy Practices, which may read:

“We may use certain information (name, address, telephone number, dates of service, age, and gender) to contact you in the future to raise money for (name of institution). We may also provide this name to our institutionally related foundation, for the same purpose. The money raised will be used to expand and improve the services and programs we provide the community.”

It is not necessary nor should an opt-out reference be included in the Notice of Privacy Practices.

**Long Answer**

*Detailed Discussion Provided by AHP Legal Counsel:*

**The final privacy regulations include fund raising “for the benefit of the covered entity” as a “health care operation.” 45 CFR § 164.501.<sup>6</sup> Covered entities do not have to obtain an authorization from the patient to use or disclose a limited subset of otherwise protected health information for the purpose of raising funds. That is to say that the use of demographic information for fund-raising purposes is permissible under the regulations. 45 CFR § 164.502(a)(1)(vi).** The relevant section states that:

(f)(1) Standards: uses and disclosures for fund raising. 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, without an authorization meeting requirements of §164.508:

- (i) Demographic information relating to an individual; and
- (ii) Dates of health care provided to an individual.

(2) Implementation specifications: fund-raising requirements.

(i) The covered entity may not use or disclose protected health information for fund-raising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by 164.520(b)(1)(iii)(B) [the Notice of Privacy Practices] is included in the covered entity’s notice;

(ii) The covered entity must include in any fund-raising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fund-raising communications.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fund-raising communications are not sent such communications. 45 CFR § 164.514(f).

A health care provider that intends to contact a patient to raise funds must include in its “Notice of Privacy Practices” a separate statement that it “may contact the individual to raise funds for the covered entity...” 45 CFR § 164.520(b)(1)(iii). From and after April 14, 2003, health care providers or other covered entities with direct patient contact must use a good faith effort to obtain a signed **Acknowledgment** of receipt of the Notice from patients at the time of the first encounter with the patient. The patient’s authorization is required to use any protected

---

<sup>6</sup> Additionally, in the comment & response section, HHS states that “[p]ermissible fund raising activities include appeals for money, sponsorship of events, etc.” However, fund raising does not include “royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc.)” This provision only applies when the entity uses protected health information for fund-raising purposes. A health care provider can still sell products using other means if it so chooses.

health information (PHI) other than dates of service or demographic information in fund raising (See Question 3).

Additionally, grateful patients who are listed on a provider's donor database prior to the compliance date need not receive individual copies of the Notice of Privacy Practices until their next encounter with the provider as a patient. At such time, the Notice of Privacy Practices must be a part of the admissions process.

You must include a fund-raising sentence in the Notice of Privacy Practices, which may read:

“We may use certain information (name, address, telephone number, dates of service, age, and gender) to contact you in the future to raise money for (name of institution). We may also provide this name to our institutionally related foundation, for the same purpose. The money raised will be used to expand and improve the services and programs we provide the community.”

It is not necessary nor should an opt-out reference be included in the Notice of Privacy Practices.

## — Question 2 — Opt-out Language

**What are examples of clauses that would fulfill the opt-out requirement in the regulations for fund-raising communications? If an individual upon receiving a fund-raising solicitation decides to opt-out from receiving additional information pertaining to fund raising, could the fund-raising entity continue to send that individual information about events if those events will have active or passive fund raising?**

### Short Answer

*Response/Conclusion:*

An opt-out provision must be included when fund-raising material is sent to former patients. An opt-out clause relating to all “further fund-raising materials” is necessary to satisfy the regulations.

#### *Sample Opt-out Language*

Please write to us at our address if you wish to have your name removed from the list to receive fund-raising requests supporting the [Name of Entity] in the future.

*The following clause could, but does not need to be included.*

In the event that you contact us with this request, all reasonable efforts will be taken to ensure that you will not receive any fund-raising communications from us in the future.

### Long Answer

*Detailed Discussion Provided by AHP Legal Counsel:*

HHS gives little guidance on what must be included in the opt-out provision. The regulations state that the covered entity must include a “description” of how the patient can opt out and the covered entity “must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fund-raising communications are not sent such communications.” § 164.514(f)(2).

The Preamble section on fund raising states that “we require fund-raising materials to explain how the individual may opt out of any further fund-raising communications, and covered entities are required to honor such requests.” *Preamble 45 CFR § 164.514(f)*. The opt-out clause should refer to all future materials relating to fund raising. Besides this brief statement, the regulations, including the Preamble and comment and response sections, do not describe what this opt-out explanation should contain, where it should be located on the fund-raising materials, or how it should be presented on this material.

A statement in the Preamble to the 2000 Final Rule has created confusion about whether some description of the opt-out is required in the Notice of Privacy Practices. The discussion in the Preamble states that “As part of the notice and in any fund-raising materials, covered entities must provide information explaining how individuals may opt out of fund-raising communications”. *See appendices.* **However, the regulations themselves in 45 CFR § 164.514(f)(2)(ii) only require the covered entity to include the opt-out explanation “in any fund-raising materials it sends to an individual”.**

The regulations also require the covered entity to include the statement in the Notice required by § 164.520(b)(1)(iii)(B), which states only that “The covered entity may contact the individual to raise funds for the covered entity.” The regulations do not require a description of the opt-out in the Notice, as long as the opt out is contained in fund-raising materials sent to an individual. Each covered entity should make its own decision about whether it includes a reference to the ability of opt-out in the Notice based on its total approach to the amount of specificity it desires in its Notice. This is the recommended way of conducting fund-raising activities.

#### Plain Language

Although the regulations do not discuss plain language requirements in this context, the use of plain language is mandated for the Notice of Privacy Practices provisions of the regulations. 45 CFR § 164.520(b). HHS has stated that a covered entity will satisfy the plain language requirements if they “make a reasonable effort to: organize material to serve the needs of the reader; write short sentences in the active voice, using you and other pronouns; use common, everyday words in sentences; and divide material into short sections. *Preamble 45 CFR § 164.520(b).* It would be prudent to comply with the plain language provisions when drafting opt-out clauses.

#### Sample Clauses

Two versions of opt-out provisions are provided as examples.

##### *Suggested Version*

Please write to us at our address if you wish to have your name removed from the list to receive fund-raising requests supporting the [Name of Entity] in the future.

##### *Longer Version*

Please write to us at our address if you wish to have your name removed from the list to receive fund-raising requests supporting the [Name of Entity] in the future. In the event that you contact us with this request, all reasonable efforts will be taken to ensure that your will not receive any fund-raising communications from us in the future.

*Please note that whether or not the second sentence in this second version is included, the requirement to use all reasonable efforts is imposed by HIPAA.*

#### Languages

The provisions in the regulations concerning opt-out clauses do not discuss the necessity of having these clauses communicated in a variety of languages. The language requirements should not apply to the opt-out provisions, unless of course the solicitation is multi-lingual.<sup>7</sup>

*Fund-raising Events*

In the event that an individual opts out under the broad version of the opt-out provision, the regulations do not discuss whether a covered entity can continue to send that individual information concerning health care provider events that may include active or passive fund raising. See the discussion on Question 5 for a more complete discussion of restrictions on marketing contained in the 2002 Final Rule.

---

<sup>7</sup> Health care providers will be required, however, to provide privacy notices in several languages. Health care providers do not normally collect demographic information on the language spoken by its patients. The Office of Civil Rights rules on communication generally apply to health care providers, and should be followed. Keep the needs of disabled patients in mind as well.

## — Question 3 — Filtering Data

**Can a health care provider filter patient information when determining to which prior patients they will send fund-raising communications? For example, can the fund raiser request a list from the health care provider that excludes psychiatric or pediatric patients? What would constitute permitted filters?**

### Short Answer

*Response/Conclusion:*

The Privacy Rule starts with the concept that the patient’s authorization is required for use or disclosure of their own PHI unless the use or disclosure is specifically permitted by the Privacy Rule, as described in the Covered Entity’s Notice of Privacy Practices. **The fundamental permitted uses and disclosures include treatment, payment for treatment, and some operations of covered entities (including fund raising); some disclosures incidental to or related to those uses; or as required or permitted by other law or a compelling public purpose.** The PHI that can be used or disclosed is generally limited to that which is the minimum necessary to accomplish the task<sup>8</sup>. *45 CFR § 164.502(b)* The minimum necessary requirement applies to the use or disclosure of PHI for any health care operation, including fund raising, but an additional limit is imposed in the regulations specifically to define the minimum necessary information for fund-raising purposes.

The limited information a covered entity can use and disclose includes dates of treatment and “demographic information” to raise funds. Demographic information is not defined in the Privacy Rule, but includes the patient’s “name, address and other contact information, age, gender, and insurance status.” HHS says that information about a patient’s illness, treatment, or services provided cannot be used for fund-raising purposes without the patient’s authorization. Use of filters to exclude or target fund-raising efforts that are based on the prohibited factors – illness, treatment or services provided – would present risk. The use of filters that do not identify a prohibited factor should be permissible within reason. For instance, the fund raiser might want to send fund raising material, but desire that the mailing list exclude all psychiatric and pediatric patients. The Health care provider should be able to filter out contact information to avoid unintended solicitation, as long as the filtering was not done in concert with other efforts which in fact produce mailing lists based on the patient’s illness, treatment or services received.

### Long Answer

*Detailed Discussion Provided by AHP Legal Counsel:*

---

<sup>8</sup> The only exceptions to the requirement to use or disclose only the minimum necessary information are for treatment of the individual and for defined disclosures required by law. The rule does not impose the minimally necessary requirement on disclosures to the individual themselves and pursuant to an authorization, but in both of those situations the individual is directly controlling his or her own health information.

Fund raising for its own benefit is defined to be part of a covered entity's health care operations. 45 CFR § 164.501. Uses and disclosures of PHI for all health care operations is subject to the requirement to use reasonable efforts to limit disclosure to the minimum necessary to accomplish the intended purpose for which the PHI will be used. 45 CFR § 164.502(b). This general rule applies to all health care operations, but the regulations go on to expressly limit the PHI that can be used for fund raising to "demographic information relating to the individual" and "dates of health care provided to an individual". 45 CFR § 164.514(f)(1). The regulations do not define "demographic information relating to the individual", but the discussion in the Preamble to the Final Rule provides a definitional framework.

HHS states that "[d]emographic information<sup>9</sup> is not defined in the rule, but will generally include [for the purpose of fund raising] name, address and other contact information, age, gender, and insurance status." *Preamble 45 CFR § 164.514(f)*. In the following exchange, HHS further clarifies the meaning of "demographic information" and the use of non-demographic information in fund raising:

*Comment:* Several commentators asked us to address the content of fund-raising letters. They pointed out that disease or condition-specific letters requesting contributions, if opened by the wrong person, could reveal personal information about the intended recipient.

*Response:* We agree that such communications raise privacy concerns. In the final rule, we limit the information that can be used or disclosed for fund raising, and **exclude information about diagnosis, nature of services, or treatment.** *Id.* (emphasis added).<sup>10</sup>

*a. Permissible Information<sup>11</sup>* Note: There is no regulatory source for this advice, other than the Preamble to the 2000 Final Rule.

Protected health information that can be utilized for fund-raising purposes without obtaining a patient's authorization includes:

- Date of Service [45 CFR § 164.514(f)(1)]
- Demographic Information 45 CFR § 164.514(f)(1) [all of the above are discussed as "demographic information" in the Preamble] to the 2000 Final Rule
- Name
- Address
- Other contact information (phone numbers, e-mail, etc.)
- Age
- Gender
- Insurance status

---

<sup>9</sup> We note that the dictionary definition of "demographic" would not support HHS' statement in the Preamble, but an administrative agency's contemporaneous pronouncement of what it intended its regulations to mean is generally afforded substantial weight. The statement in the Preamble is the only definition available.

<sup>10</sup> Of course, such information could be used with the patient's authorization. This Memo assumes that authorization will not be sought in the great majority of cases. We note again that this list of impermissible items is found only in the Preamble, and is not found in the regulation itself.

<sup>11</sup> The Privacy Rule was proposed in 1999 and initially adopted as a final rule in December 2000 at 65 Fed. Reg. 82461-82829 (12-28-2000) ("the 2000 Final Rule"). Substantial amendments were proposed in March, 2002, and an amended final Privacy Rule was adopted in August 2002 (the "2002 Final Rule"). The fund-raising provisions were not amended in the 2002 Final Rule, and there is no discussion of the fund-raising issue in the Preamble to the 2002 Final Rule. Therefore, guidance on fund raising is found primarily in the Preamble to the 2000 Final Rule, pertinent parts of which are appended to this document.

*b. Impermissible Use and Disclosure*

PHI that cannot be used without a patient first signing an authorization includes:

- Diagnosis
- Nature of services
- Treatment
- Place within health care provider where patient receives treatment that identifies the treatment, such as:
  - Department of Psychiatry
  - Department of Obstetrics
  - Department of Radiation Oncology

*c. Questionable Use and Disclosure*

Although not discussed in the regulations or any of the lengthy Preambles to any of the proposed or adopted regulations, a covered entity may be able to use information about the department in which the patient was treated to filter patient names for fund-raising purposes if the department name does not identify the type or nature of treatment. **For example, when a patient is treated by the medical/surgery or another type of general department, using or disclosing this information for fund-raising filtration purposes would not appear to reveal the diagnosis or nature of the services or treatment received by the affected individuals, and would appear to fit within the minimum necessary information to accomplish the goal — fund raising.**

A covered entity should adopt policies that address by job title the types of PHI that can, or can not be used in connection with the day-to-day performance of various job functions. Adoption of such policies and procedures eliminates the need to make case specific decisions of whether and how much PHI can be used or disclosed in normal, day-to-day operations. A policy could be structured to ensure that fund raisers received only limited PHI as described in this Memorandum, while giving them the right to request some other department of the health care provider to review patient PHI to ensure that data received fit within the limitation. The use of appropriate filtering by individuals whose job entailed access to a broader spectrum of PHI in order to ensure that the fund raiser did not receive inappropriate information would appear to be consistent with the general duty of the health care provider to use reasonable efforts to limit use of PHI to the minimum necessary to accomplish the task.

As we understand it, the purpose of such limited filtering would generally be to avoid sending fund-raising materials to recipients who could reasonably be anticipated not to be interested in receiving them (e.g., psychiatric patients). This type of filtering would further the purpose of disclosing only the minimum necessary health information to accomplish the desired goal – in this case, contacting patients for fund raising. Filtering should never be done in such a way that impermissible PHI is disclosed – i.e., successive filtering that resulted in a patient list limited to, for instance, obstetrics patients.

**Caution:** We also must caution that the adopted privacy rules do not preempt state laws that are more restrictive than the federal rules, or other federal laws. For instance, HIPAA permits limited, traditional disclosure of health care provider directory information, but other federal law prohibits a health care provider from even responding to an inquiry about a patient

receiving treatment for substance abuse, and the particular state law on the privacy of medical records must be considered by the fund-raising entity. However, the most essential information – name, age, gender, date of treatment, and address – can be used safely for fund-raising efforts.

*Remember the Notice*

The final rule requires providers with a direct treatment relationship such as a health care provider to offer a Notice to each patient upon the first direct encounter following the effective date of the Privacy Rule, April 14, 2003, and to use reasonable efforts to obtain a written acknowledgment from the patient that the Notice was offered. The Health care provider must develop and maintain a system to identify patients who have received the Notice of Privacy Practices.

## — Question 4 — Institutionally Related Foundation, Business Associates

### Do the regulations require that a covered entity have a formal “business associate” type contract with an institutionally related foundation?

#### Short Answer

#### Response/Conclusion:

A business associate agreement is not required with an institutionally related foundation. Because in the regulations, the institutionally related foundation is a part of health care operations. As a part of health care operations, a business associate agreement is not required.

The Preamble discussion indicates that a health care provider can disclose patient information from a health care provider to an institutionally related foundation without a business associate agreement. A health care provider could either 1) include the foundation in its Notice of Privacy Practices and not use a business associate agreement; 2) use a business associate agreement; or 3) rely on the Preamble language discussed below while avoiding either 1 or 2.

The regulations do not expressly require that a covered entity have a formal “business associate” type contract with an institutionally related foundation.<sup>12</sup> In fact AHP’s successful educational efforts with HHS resulted in the inclusion of the institutionally related fund raiser as a part of health care operations. Therefore, no business associate agreement is needed. It is necessary that the entity performing fund-raising duties meet the definition of an institutionally related foundation, described by HHS as:

[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. *Preamble to the 2000 Final Rule 45 CFR § 164.514(f)*

This definition would appear to cover almost all traditional nonprofit fund-raising entities affiliated with a health care provider, which are generally formed as supporting organizations under §509(a)(3) of the Code, or as public charities under § 509(a)(1), even if the supporting health care provider was not the only recipient of its support.<sup>13</sup>

---

<sup>12</sup> Unlike the obligations imposed on a business associate, there is no express requirement that the covered entity must have a contract with an institutionally related foundation, which would impose the privacy regulations on the foundation. However, it would be problematic for a covered entity if an institutionally related foundation failed to comply with the privacy regulations. Therefore, the operating imperative should be that institutionally related foundations comply with the privacy regulations.

<sup>13</sup> The Preamble gives examples of entities that would qualify as institutionally related foundations, to include “a nonprofit foundation established for the specific purpose of raising funds for “[a] health care provider and a foundation that has as its mission the support of the members of a particular health care provider chain that includes the covered health care provider.” The Preamble adopts the common understanding that a fund-raising foundation closely associated with one or more health care providers named in its charter is an institutionally related foundation. *Preamble 45 CFR § 164.514(f)*.

HHS has concluded that “[t]he term does not include 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, because its charitable purpose is not specific to the covered entity.” *Id.* This distinction is critical, but would generally not impact traditional health care provider foundations.<sup>14</sup>

#### Fund Raising by a Business Associate

If the fund-raising entity (a firm or fund-raising services provider) is not part of the health care provider, or its institutionally related foundation, it must enter into a business associate contract with the health care provider that meets regulatory standards, if any patient information will be released to the entity. Similarly, an institutionally related foundation should insist on a business associate contract with any consultant it retains if the consultant is provided access to patient information.<sup>15</sup> Through this contract, the business associate becomes subject to some of the obligations mandated by the Privacy Rule. The covered entity (i.e., the Health care provider) is not liable under HIPAA should the business associate fail to comply with the Privacy Rule, but it must take reasonable action if it learns that the business associate is not in compliance. HHS provided a sample business associate addendum when it published the final rule which can be used as a starting point in preparing any business associate agreement a covered entity may wish to use. [See *sample agreement attached or visit <http://www.hhs.gov/ocr/hipaa/contractprov.htm>*].

#### Long Answer

*Detailed Discussion Provided by AHP Legal Counsel:*

We do not believe that a business associate agreement between a health care provider and its institutionally related foundation is required. That belief is founded in statements in the Preamble to the 2000 Privacy Rule, and the regulations themselves are not as clear as they could be.

In the general discussion in the Federal Register when the 2000 Final Rule was adopted, HHS stated that:

As provided in §164.514(f) and described in detail in the corresponding Preamble, authorization is not required when a covered entity uses or discloses demographic information and information about dates of health care provided to an individual for the purpose of raising funds for its own benefit, **nor when it discloses such information to an institutionally related foundation to raise funds for the covered entity.** (emphasis added) [*Preamble to the 2000 Final Rule.*]

In its specific discussion on the newly added §164.514(f), HHS added further clarification:

<sup>14</sup> The American Cancer Society and the United Way, for example, are not institutionally related foundations. Presumably, a foundation dedicated to raising funds to support the children’s health care provider of a major teaching health care provider would be.

<sup>15</sup> A business associate contract must: “[e]stablish the permitted and required uses and disclosures of [protected health information] by the business associate.” § 164.504(e) (2) (i). “[a]uthorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract § 164.504(e) (2) (iii) and require the business associate to comply with the HIPAA requirements.

We permit a covered entity to disclose the limited protected health information to a business associate for fund raising on its own behalf. **We also permit a covered entity to disclose the information to an institutionally related foundation.** (emphasis added)

This distinction between a business associate and a foundation is repeated in the regulation itself. Section 45 CFR 164.514(f)(1) states that:

“Standard: uses and disclosures for fund raising. 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, without an authorization meeting the requirements of §164.508:

- (i) Demographic information relating to an individual; and
- (ii) Dates of health care provided to an individual.” (emphasis added)

There would be no reason to differentiate in both the Preamble and in the regulation if the institutionally related foundation were merely a business associate, because the regulations describing the business associate relationship would have simply applied to the foundation. HHS differentiated between a business associate and a foundation, leading to the clear inference that a covered entity would not be required to treat a foundation as a business associate. The Preamble discussion goes on to discuss both the meaning of and some of the reasoning for differentiation between foundation and business associate, and makes clear that the distinction was not accidental:

We agree with commentators that our proposal could have adversely effected charitable giving, and accordingly make several modifications to the proposal. First, the final rule allows a covered entity to use or disclose to a business associate protected health information without authorization to identify individuals for fund raising for its own benefit.

Second, the final rule allows a covered entity to disclose protected health information without authorization to an institutionally related foundation that has as its mission to benefit the covered entity. **This special provision is necessary to accommodate tax code provisions which may not allow such foundations to be business associates of their associated covered entity.** (emphasis added)

The Preamble also discusses what kinds of entities may qualify as foundations. Unfortunately, although the regulations themselves expressly permit disclosure of protected health information (PHI) to such foundations, they neither define foundations nor specifically exclude them from the definition of “business associate.” As noted, there is no further discussion on the status of foundation or on fund raising in general in any of the subsequent Federal Register issuances, or in the “FAQ” that HHS released in December, 2002 on the Privacy Rule.

Therefore, those who read the regulations without the benefit of the language in the Preamble to the 2000 Final Rule would be likely to reach the conclusion that a business associate agreement is required, because in almost any other circumstance a covered entity could not disclose PHI to an independent entity in the absence of such an agreement. We believe the

language in the Preamble is clear enough to justify the disclosure of PHI to a foundation without having a business associate contract in place, although the foundation, as a sort of alter ego to the covered entity, should certainly comply with the confidentiality provisions of the Privacy Rule. The Preamble language, published at the time HHS adopted the regulation for the first time, is entitled to great weight in interpreting the regulations. The covered entity could also elect to simply include the affiliated foundation in its Notice of Privacy Practices to bring it clearly within the covered entity. This could be accomplished by defining it as part of the “we” in the Notice of Privacy Practices. This would have the practical effect of treating the foundation as if it were part of the covered entity for purposes of HIPAA compliance.

## — Question 5 — Newsletters, Patient Education

**What effect will the regulations have on marketing efforts such as the distribution of newsletters, seminars, patient education, and health fairs?**

### Short Answer

*Response/Conclusion:*

Although the main concern for AHP is fund raising, it is important to understand how the final regulations will effect marketing.

The 2002 Final Rule requires the patient's authorization to use any PHI in connection with marketing, except for face-to-face communications and use of promotional gifts with a nominal value. Marketing is no longer defined as part of health care operations<sup>16</sup>, meaning that marketing efforts (in the absence of authorization, which is impracticable) must either be based on information that is not PHI or fit within one of the carve outs described below. Covered entities should take care in the use of directed communications or newsletters to have the contents either fall outside the definition of marketing, or avoid using PHI to target the recipients.

The marketing rules have caused confusion. Some guidelines may help:

1) A health care provider can not disclose PHI to another entity for the purpose of that entity's marketing.

2) A health care provider is not "marketing" under HIPAA when it describes the services and products it offers. Therefore, a health care provider can use a PHI derived mailing list to send communications describing its own products or services. The Office of Civil Rights of HHS gave the following example in its December 3, 2002 FAQ release:

A health care provider [can] use its patient list to announce the arrival of a new specialty group (e.g., orthopedic) or the acquisition of new equipment (e.g., x-ray machine or [MRI]) through a general mailing or publication.

3) Similarly, a communication is not marketing under HIPAA if it is made for treatment or for operations (e.g., recommending alternative treatments, case management or care or for co-ordination, etc.)

4) If a business associate is used to perform permitted marketing, it must agree not to use the PHI for its own or anyone else's purpose.

---

<sup>16</sup> Marketing was so defined in the 2000 Final Rule, which permitted more generous use of PHI for marketing than is the case under the 2002 Final Rule.

5) Generally, health promotion and wellness programs do not fall under the HIPAA definition of marketing. The FAQ approves the example of a health care provider sending a flyer about its new weight-loss program to all patients who were defined as obese, even if the treatment received was not specifically for obesity.<sup>17</sup>

The issue can be avoided by using mailing lists that are not derived from the health care provider's patient lists for newsletters and similar widely disseminated mailings that contain marketing that does not fit within one of the carve-outs discussed above. HIPAA forbids the use or disclosure of PHI (including the names and addresses of patients) for marketing, but other sources of mailing lists are available.

### Long Answer

*Detailed Discussion Provided by AHP Legal Counsel:*

Although the main area of concern for AHP is fund raising, it is important to understand how the final regulations will affect marketing efforts. The 2000 Final Rule permitted the use of PHI in marketing without the patient's consent pursuant to an opt-out provision similar to that required for fund raising. Newsletters and similar items were not required to contain an opt out.

However, in the 2002 Final Rule the marketing provisions were substantially amended. The Final Rule requires the patient's authorization to use any PHI in connection with marketing, except for face-to-face communications and use of promotional gifts with a nominal value. 45 CFR 164.508(a) (3). The example used by the Office of Civil Rights to explain this exception is a health care provider providing "a free package of formula and other baby products to new mothers as they leave the maternity ward". Marketing is defined as any communication about a product or service that encourages the recipient to buy or use the good or service, with limited carve outs. 45 CFR § 164.501. The carve outs are important, but the line between marketing (which requires the patient's authorization if their PHI will be used in, for instance, a marketing mailing list) and treatment can be blurred.

**Marketing is no longer defined as part of health care operations.** Since use or disclosure of PHI without authorization is effectively limited to uses for treatment, payment or health care operations, there is no exception under HIPAA available for pure marketing. The result is that most marketing efforts (in the absence of authorization, which is impracticable) must either be based on information that is not PHI (i.e., not based on a mailing list of patients), or fall within one of the categories of carve outs discussed below. Covered entities should take care in the use of directed communications or newsletters to either fall outside the definition of marketing or avoid using PHI to target the recipients.

Marketing is defined in the Privacy Rule as:

(1) to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

---

<sup>17</sup> The HIPAA rules do not amend the Civil Monetary Penalty restrictions on offering inducements to Medicare and Medicaid beneficiaries, which should also be reviewed if beneficiaries are offered such programs.

(i) To describe a health-related product or service ...that is provided by ... the covered entity making the communication,....

(ii) For treatment of the individual; or

(iii) For 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.

(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service. 45 CFR

§164.501

Additional guidance was recently provided in the Frequently Asked Questions (FAQ) released on December 3, 2002 by the Office of Civil Rights of HHS. This guidance attempts to explain what is and is not permitted without authorization. Exerpts are given below:

What is NOT “Marketing”? The Privacy Rule carves out exceptions to the definition of marketing under the following three categories:

- (1) A communication is not “marketing” if it is made 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:
  - A health care provider uses its patient list to announce the arrival of a new specialty group (e.g., orthopedic) or the acquisition of new equipment (e.g., x-ray machine or magnetic resonance image machine) through a general mailing or publication.

The Frequently Asked Questions provide this additional guidance, with an additional warning. Basically, if something fits a carve out as a treatment communication or description of the entity’s own services, it is permitted, and the covered entity can use PHI in making communications that would otherwise constitute marketing within the broad definition contained in the Privacy Rule. However, if the covered entity is wrong, then the communication is simply marketing and the health care provider would have committed a violation if PHI (e.g., a patient list) was used to send the communication as the following FAQ illustrates.

**Q: How can I distinguish between activities for treatment or health care operations versus marketing activities?**

**A:** The overlap among common usages of the terms “treatment,” “healthcare operations,” and “marketing” is unavoidable. For instance, in recommending treatments, providers and health plans sometimes advise patients to purchase goods and services. Similarly, when a health plan explains to its members the benefits it provides, it too is encouraging the use or purchase of goods and services.

The HIPAA Privacy Rule defines these terms specifically, so they can be distinguished. **For example, the Privacy Rule excludes treatment communications and certain health care operations activities from the definition of “marketing.”** If a communication falls under one of the definition’s exceptions, the marketing rules do not apply. In these cases, covered entities may engage in the activity without first obtaining an authorization. See the fact sheet on this web site about marketing, as well as the definition of “marketing” at 45 CFR 164.501, for more information.

**However, if a health care operation communication does not fall within one of these specific exceptions** to the marketing definition, and the communication falls under the definition of “marketing,” the Privacy Rule’s provisions restricting the use or disclosure of protected health information for marketing purposes will apply. For these marketing communications, **the individual’s authorization is required before a covered entity may use or disclose protected health information.** (emphasis added)

The FAQ provides more useful guidance when it explains that wellness programs and preventative care do not generally fall within the definition of marketing.

**Q: Do disease management, health promotion, preventive care, and wellness programs fall under the HIPAA Privacy Rule’s definition of “marketing”?**

**A: Generally, no.** To the extent the disease management or wellness program is operated by the covered entity directly or by a business associate, **communications about such programs are not marketing because they are about the covered entity’s own health-related services. So, for example, a health care provider’s Wellness Department could start a weight-loss program and send a flyer to all patients seen in the health care provider over the past year who meet the definition of obese, even if those individuals were not specifically seen for obesity when they were in the health care provider.**

Moreover, a communication that merely promotes health in a general manner and does not promote a specific product or service from a particular provider does not meet the definition of “marketing.” Such communications may include population-based activities in the areas of health education or disease prevention. Examples of general health promotional material include mailings reminding women to get an annual mammogram; mailings providing information about how to lower cholesterol, new developments in health care (e.g., new diagnostic tools), support groups, organ donation, cancer prevention, and health fairs.

**Q: Is it “marketing” for a covered entity to describe products or services that are provided by the covered entity to its patients, or to describe products or services that are included in the health plan’s plan of benefits to members of the health plan?**

**A: No.** The HIPAA Privacy Rule excludes from the definition of “marketing” communications made to describe a covered entity’s 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. Thus, it would not be marketing for a physician who has developed a new anti-snore device to send a flyer describing it to all of her patients (whether or not each patient has actually sought treatment for snoring). Nor would it be marketing for an ophthalmologist or health plan to send existing patients or members discounts for eye-exams or eyeglasses available only to the patients and members. Similarly, it would not be marketing for an insurance plan to send its members a description of covered benefits, payment schedules, and claims procedures.

## —Definitions— Notice of Privacy Practice and Opt Out

**Notice of Privacy Practices:** According to the final Privacy Rule, health care institutions that have a direct treatment relationship with an individual must provide the Notice by the date of the first service encounter on or after April 14, 2003; and make a good faith effort to obtain the patients' written acknowledgement of having received a Notice of Privacy Practices. The Notice must be written in plain language and include a sentence about contacting individuals to raise funds for the institution. In the absence of a direct encounter, the patient's signed acknowledgement is not necessary.

Your institution's Notice of Privacy Practices is a statement that outlines how medical record information will be used and the limitations upon its use. A covered entity may not use or disclose PHI in a way that is not mentioned in the Notice. Relative to philanthropy, the Notice of Privacy Practices must contain a sentence about contacting individuals to raise funds. The regulations impose many specific requirements, and care must be taken in drafting the Notice. The Notice of Privacy Practices must be made available to patients. Your institution must post the Notice of Privacy Practices on its Web site and make it available electronically, and post it in prominent places inside the institution. You can also include it in newsletters or other communication vehicles. You do not have to mail the Notice of Privacy Practices to patients prior to sending a fund raising soliciting to them, although the Notice must be in place and available prior to April 14, 2003. This is a common misunderstanding. While many of your compliance officers or others in this position may suggest or even recommend that you mail the Notice of Privacy Practices before soliciting patients, this is not required or necessary. You must post the Notice and make it available and provide a paper copy on request. You should anticipate an increase in media attention to the Privacy Rule as the effective date comes closer, and you should participate in your institution's Privacy Rule roll out to ensure that fund-raising efforts are not harmed through oversight or inadvertence.

Additionally, grateful patients who are listed on a provider's donor database prior to the compliance date need not receive individual copies of the Notice of Privacy Practices until their next encounter with the provider as a patient. At such time, the Notice of Privacy Practices must be a part of the admissions process.

You must include a fund-raising sentence in the Notice of Privacy Practices, which may read:

“We may use certain information (name, address, telephone number, dates of service, age, and gender) to contact you in the future to raise money for (name of institution). We may also provide this name to our institutionally related foundation, for the same purpose. The money raised will be used to expand and improve the services and programs we provide the community.”

It is not necessary nor should an opt-out reference be included in the Notice of Privacy Practices.

**The Opt-out Requirement:** An opt-out clause relating to fund-raising materials must be included in all solicitations to satisfy the regulations, and must be included in all of your solicitations. The sample version that AHP suggests, and our legal counsel reviewed, states:

“Please write to us at our address if you wish to have your name removed from the list to receive fund-raising requests supporting (name of entity) in the future.”

This is a direct and simple statement that satisfies the “opt-out” requirement in the regulations.

You must also institute a system that will track opt-outs and follow up to ensure that any individual that has opted out is in fact removed from fund-raising mailing lists.

## —Definitions— Important Terms

**This section presents selected major terms defined in the Privacy Rule. Familiarity with these terms will greatly contribute to your understanding of HIPAA.**

**Authorization.** Authorization is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. An Authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual. An Authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an Authorization.

**Business Associate.** A Business Associate is any person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides service to, a covered entity. Business Associate functions and activities include claims processing or administration, data analysis processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business Associate services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services.

**Business Associate Agreement.** The Privacy Rule mandates that covered entities have a Business Associate Agreement with each of their business associates. The Business Associate Agreement must (i) describe the permitted and required uses of protected health information by the business associate, (ii) provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by

law, and (iii) require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

**Covered Functions.** Covered Functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

**Covered Entity.** Covered Entity means (1) a health plan, (2) a health care clearinghouse, or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.

**Disclosure.** Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

**Health Care.** Health Care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

**Health Care Clearinghouse.** Health Care Clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions: (1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

**Health Care Operations.** Health Care Operations are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. **Fund raising is defined to be part of a covered entity’s operations.**

**Health Care Provider.** Health Care Provider is any individual or organization that furnishes, bills, or is paid for furnishing health care services in the normal course of business.

**Health Information.** Health Information means any information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) related 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.** HHS stands for the Department of Health and Human Services. Within HHS, the Office of Civil Rights (“OCR”) is charged with the responsibility of enforcing the Privacy Rule.

**Individual.** Individual means the person who is the subject of protected health information.

**Individually Identifiable Health Information.** Individually Identifiable Health Information (“IIHI”) is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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 (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**Institutionally Related Foundation.** Institutionally Related Foundation is a foundation that qualifies as a nonprofit charitable foundation under § 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 provider in its community.

**Marketing.** Marketing means making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Generally, if the communication is marketing, and does not fall within the carve outs discussed in the Memorandum, the communication can occur only if the covered entity first obtains an individual’s authorization.

**Minimum Necessary Standard.** The Minimum Necessary Standard requires covered entities to evaluate their practice and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the Minimum Necessary to accomplish the intended purpose. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the Minimum Necessary requirements.

**Notice of Privacy Practices.** The HIPAA Privacy Rule gives individuals a fundamental new right to be informed of the privacy practices of their health plans and of most of their health care providers, as well as to be informed of their privacy rights with respect to their personal health information. Health plans and covered health care providers are required to develop and make available a Notice of Privacy Practices that provides a clear explanation of these rights and practices. The Notice is intended to focus individuals on privacy issues and concerns, and to prompt them to have discussions with their health plans and health care providers and exercise their rights.

**Payment.** Payment encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill

their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

**Privacy Officer.** The Privacy Officer is the person designated by the covered entity 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.

**Protected Health Information.** Protected Health Information means individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in any medium described in the definition of electronic media; or (iii) transmitted or maintained in any other form or medium. Protected Health Information excludes individually identifiable health information in educational records covered by the Family Educational Rights and Privacy Act ("FERPA") and employment records held by a covered entity in its role as employer.

**Required By Law.** Required By Law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information that is enforceable in a court of law. Required By Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, 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 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.** Secretary refers to the Secretary of Health and Human Services or his or her designee.

**TPO.** TPO stands for treatment, payment, and health care operations. Under the regulations, fund raising is a part of health care operations.

## — Sample Business Associate Contract Provisions —

Provided by the U.S. Department of Health and Human Services Office of Civil Rights  
<http://www.hhs.gov/ocr/hipaa/contractprov.htm>

# Medical Privacy - National Standards to Protect the Privacy of Personal Health Information

**SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS**  
(Published in FR 67 No.157 pg.53182, 53264 (August 14, 2002))

### Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

### Sample Business Associate Contract Provisions<sup>1</sup>

#### Definitions (alternative approaches)

##### Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

- a. Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].
- b. Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].
- c. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
- d. Privacy Rule. "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.
- e. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- f. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.
- g. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

#### Obligations and Activities of Business Associate

- a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
- b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]
- d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
- e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

- f. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]
- g. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]
- h. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- i. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.
- j. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

#### Permitted Uses and Disclosures by Business Associate

#### General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

a. Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:  
[List Purposes].

b. Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

- a. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- c. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B).
- d. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

- a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
- b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
- c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45

CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

#### Permissible Requests by Covered Entity

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 the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

#### Term and Termination

- a. Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]
- b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
  1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the \_\_\_\_\_ Agreement/ sections \_\_\_\_ of the \_\_\_\_\_ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
  2. Immediately terminate this Agreement [and the \_\_\_\_\_ Agreement/ sections \_\_\_\_ of the \_\_\_\_\_ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or
  3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

[Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

#### c. Effect of Termination.

1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business

Associate shall retain no copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

### Miscellaneous

- a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
- b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- c. Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.
- d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

<sup>1</sup> *Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.*

*Last revised: August 14, 2002*