When Federal Privacy Rules and Fundraising Desires Meet: An Advisory on the Use of Protected Health Information in Fundraising Communications

Purpose

This compliance advisory addresses the HIPAA Privacy Rule[1] requirements for the use, disclosure and sharing of Protected Health Information (PHI) for fundraising communications. The Advisory assumes that the reader has an understanding of the HIPAA Privacy Rule and would benefit from an in-depth discussion of the rule's requirements related to fundraising. The first section of the Advisory is in a Question and Answer format that provides quick answers to common questions about HIPAA requirements and fundraising. The second section is an in-depth discussion that is an excellent resource for more detailed information and includes suggested templates for communicating with patients, cites to Federal statutes and regulations, and relevant HIPAA definitions.

The information provided is meant to be advisory. Readers are advised to consider their own compliance environment and seek specific legal advice from their institution's counsel prior to implementing the suggestions contained herein. It is also important to become familiar with your state's requirements, which may be more stringent than those of Privacy Rule. However, a discussion of state-level privacy/confidentiality rules related to fundraising is outside the scope of this advisory.

Questions and Answers: HIPAA Privacy Requirements and Fundraising Communications

1. ***What is "Fundraising"?***

A communication by or on behalf of a Covered Entity for the purpose of raising funds for a Covered Entity, including, donations, appeals, or sponsorship of events, but not royalties or remittances for sale of products.

2. ***Do the HIPAA provisions on fundraising apply to all fundraising communications by or on behalf of a Covered Entity?***

No.

The Final Rule provisions apply to the use or disclosure of PHI for fundraising communications. Fundraising communications by a Covered Entity based solely on non-PHI sources of information, such as a purchased mailing list, alumnus or employee information, or direct contact initiated by a potential donor, are not subject to the Final Rule provisions.

[1] The HHS Office of Civil Rights (OCR) enforces the HIPAA Privacy regulation. A compilation of resources, including links to the statute, regulations, and FAQs is available on the OCR site at http://www.hhs.gov/ocr/privacy/

3. ***What is the scope of fundraising communications?***

Fundraising communication is a solicitation for funds, whether in writing or oral. An acknowledgement or thank you letter for receipt of donation or update of current development project without request for additional donation would not be a fundraising communication. An event invitation that includes request of a donation to attend would be a fundraising communication.

4. ***Can I use PHI for Fundraising Purposes?***

Yes, provided that all HIPAA requirements are met.

If a Covered Entity's Notice of Privacy Practices provides that the entity may contact the patient for fundraising and the patient has a right to opt-out of fundraising communications, then ***Permitted Fundraising PHI*** may be used for fundraising communications.

5. ***What PHI may a Covered Entity use for fundraising communications?***

Under the Final Rule, a Covered Entity may use ***patient*** demographic, health status data and dates of health service for fundraising purposes. The Permitted Fundraising PHI that may be used is the following:

**Name	**General Department of service
**Address and other contact information	** Treating physician information
** Email address	** Age
** Gender	**Health insurance status
** Dates of patient's health care services	**Outcome information (to screen out only)

A Covered Entity must also review applicable state privacy/confidentiality statutes or regulations that may be more restrictive. If a Covered Entity wants to use any other types of PHI, a specific written authorization from the patient must first be obtained.

6. ***Are there any types of PHI that are given extra protection under applicable federal or state regulations?***

Yes.
Special consideration should be contemplated for the following;

Mental Health, Psychotherapy Notes, Substance Abuse
Communicable Diseases, sexually transmitted infections, HIV/AIDS
Genetic Testing
Infertility treatment
Abuse, including pediatric, adult with disability, elder abuse, sexual assault
Other applicable state provisions

Due to the sensitive nature of these treatments, additional federal and state authorization requirements must be considered prior to using for fundraising communications. It is recommended that legal counsel be consulted prior to obtaining a patient's authorization for this type of information.

7. ***May a treating physician use PHI obtained during course of treatment to request donations from his patients?***

No.
All Covered Entity staff must comply with the Final Rule. Staff may only use the Permitted Fundraising PHI to communicate with patients related to fundraising communications.

8. ***Can Development staff who work with specific physicians be given a list of patients with higher disposable income to review with physicians as to appropriateness for fundraising?***

Yes.
Development staff can obtain Department listing of patients, pair Permitted Fundraising PHI with a commercial dataset and work with Chair, Committee or treating physicians to identify patients to approach for fundraising. Physicians cannot provide additional PHI to the Development staff, such as demographic identifiers that are not listed in the Final Rule or diagnostic information. If a physician shares such information inadvertently, the Development staff may not use it in any fundraising communication with the patient. The physician may nonetheless indicate the treatment outcome and whether they believe it appropriate to approach a given patient.

9. ***How does the Privacy Rule define Department of Service?***

The Final Rule permits broad designations, but does not clarify further. We have interpreted this to allow designations, such as surgery or oncology, and other fairly broad thematic area designations, but not narrower designations or information relating to diagnosis, nature of services, treatment received by the patient or specialty of treating physician. Each Covered Entity will need to review their department/division designations to determine which meet the general department of service designation. For example, a pediatric hospital may have a Department of Pediatrics and within that department many divisions such as cardiology and oncology. Since the divisions are the equivalent of general department of service, it would be allowable to use the division designation for fundraising communications targeted to patients of such division.

Any program designation below a division, however, may not be allowable since it may identify a patient's diagnosis. For example, using the Division of Cardiology within the Department of Pediatrics would be allowable, but it would not be allowable to target the Heart Transplant program. Information about a patient's diagnosis or specialized treatment program may only be used in fundraising communications with prior written authorization of the patient even if the fundraising appeal is initiated by the department or provider of service who already is aware of this information due to their treatment relationship with the patient.

A Best Practice for fundraising communications is that the definition of "Department of Service" be limited to the general divisions within a department.

10. ***How can a Covered Entity use the patient's outcome information?***

The Final Rule clarifies that outcome information includes information regarding the death of the patient or any sub-optimal result of treatment or services. In permitting its use for fundraising communications,

the intention is that the information be used to screen for those patients experiencing a sub-optimum outcome and eliminate them from fundraising solicitations.

11. ***How do patient care staff provide patient's contact information to Development staff when a patient expresses desire to donate?***

Staff may obtain verbal permission from the patient to be contacted directly by the Development Office. The Development staff should document such referral, origin of referral and patient's verbal consent to the physician/staff within the Development Office's database/donor files.

Opt-out Process

12. ***Does an opt-out provision have to be included in all Fundraising Communications?***

Yes.
All Covered Entity's fundraising communications must include, in a clear and conspicuous manner, the opportunity for the recipient to opt-out of receiving any future fundraising communications. However, a Covered Entity is not required to send a communication permitting a patient to opt-out of fundraising communication prior to the first fundraising communication if the Notice of Privacy Practices contains notice about use of PHI for fundraising and patient's ability to opt-out. Whatever method is provided for an opt-out, it must not impose an undue burden on the patient.

13. ***Can a Covered Entity require the patient to opt-out by submitting a request by mail?***

Yes, in some cases.
The Opt-out method must be "simple, quick and inexpensive" and not place undue burden on the patient. Mailing a letter places undue burden on the patient while mailing a pre-printed, pre-paid postcard provided by a Covered Entity or emailing a request to a Covered Entity does not; therefore the latter method is acceptable.

14. ***During a phone solicitation how do I inform the recipient of the opportunity to "opt-out" of receiving any future fundraising communication? Does this need to be done each time I speak with the prospective donor? Do I need to document this oral "Opt-out" notice?***

Similar to written fundraising communications, fundraising over the phone clearly must inform patients that they have a right to opt-out of further solicitations. If this hasn't been discussed or mentioned by the recipient during the call, then at the end of the telephone solicitation, consider: *"Thank you so much for your time and generosity! Please remember that you can elect not to receive any future calls or mailings from us. Just let us know if you prefer that we not contact you regarding any further fundraising efforts."* If the patient verbally opts out, the "opt-out" should be documented according to the entity's process. The opt-out must be tracked so that no future fundraising communications are made by mail, phone, email, etc. Once a donor has agreed to provide a gift, ongoing communication between staff and the donor to work out the details of that gift does not require further opt-out notice in subsequent communications. Approaching a donor for a subsequent donation, however, would require Development staff to inform the donor of their right to opt-out of additional fundraising communications.

15. ***Can the opt-out be limited to a patient fundraising drive?***

Yes.
A Covered Entity has discretion to establish an opt-out process for a patient drive or all fundraising communications. A Covered Entity must establish clear, consistent opt-out instructions that are communicated to the patients, including the consequences of opting out. A Covered Entity must implement data management systems to accurately and timely track patients' requests and implement patient's opt-out choices.

16. ***What does "conspicuous and clear" opt-out notice mean?***

It is advisable at a minimum to use the same size font as is used in the rest of the document and the notice must be in simple, plain language. Best Practice is to display a separate statement in the communication, e.g., footer, use larger, bold and/or in different color font.

17. ***Is there a time limit for the Opt-out?***

No.
The Final Rule is clear that there is to be no expiration of the opt-out decision made by the patient. Only if the patient makes an active decision to opt back in (i.e., notify the entity, preferably in written communication) is a Covered Entity allowed to include the patient back in its fundraising communications. The patient's choice to provide an additional gift is not a revocation of the opt-out request.

18. ***What does a Covered Entity or their Development staff do if a patient opts out of receiving Fundraising Communications?***

When a patient elects not to receive any further fundraising communications, the Development staff should remove the patient from the fundraising communication list and must not send any future fundraising communications to the patient. A Covered Entity must implement the opt-out process upon receipt of the patient's request. A Covered Entity must establish processes toaccurately and timely process and apply such opt-out requests. Moreover, if a clinical department is engaged in fundraising communications, the best practice is to coordinate such communications with the Development Department to ensure no patients that have opted out receive future fundraising communications.

19. ***If a patient opts out of all Fundraising Communications, can a Covered Entity continue to send notice of education or awareness events that do not include fundraising?***

Yes.
A Covered Entity may continue to send education and awareness materials that do not include fundraising. For example, communications about disease management, health promotion, wellness programs, or new services that are not funded by third parties would be acceptable. A Covered Entity would be required to comply with other applicable provisions of the Privacy Rule, such as marketing requirements.

20. ***Can patients opt back into receiving Fundraising Communications?***

Yes.
A Covered Entity may implement a process to require the patient to provide notice of the revocation of his/her opt-out which can be by any number of methods, such as phone call, e-mail, or letter. Documentation of the opt-in is essential. If a Covered Entity permits a patient to revoke an opt-out verbally, it is prudent to send an acknowledgement letter of receipt of request and to ask the patient to send back a signed acknowledgement of the desire to opt-in.

Fundraising as part of Covered Entity's Health Care Operations

21. ***Can Development staff use PHI to perform support services for Development?***

As the Privacy Rule specifically includes fundraising in the definition of Health Care Operations, some Covered Entities identify their internal fundraising operations as part of their healthcare operations. Under this interpretation, activities could include providing reports to support event planning and prospect research. These Covered Entities then allow the use of the minimum necessary PHI by certain Development Department staff to perform business activities that support its fundraising operations. The reports produced as part of the fundraising operations activities and disseminated to Development staff must contain only the Permitted Fundraising PHI data elements.

22. ***Does the Development Office need to establish a secured database of PHI used for operations activities?***

Yes.
Pursuant to the minimum necessary requirements, the Development Department must limit access to its database to staff members with a "need to know" to perform job responsibilities and must implement security controls of databases containing ePHI in accordance with the HIPAA Security Rule.

Donors as Patients

23. ***Should Development staff initiate a visit with a Donor who is in the hospital to receive services if the visit is to include fundraising communications?***

No. Development staff should not initiate visits with a new potential donor or an existing donor for fundraising communications while the patient is in the facility for the purpose of receiving health care services.

24. ***May Development staff assist a Donor to obtain appointments without an authorization?***

Yes.
Development staff may act as a conduit to scheduling staff.

Use and Disclosure of PHI for Fundraising

25. ***With whom can I share PHI for fundraising communications?***

Permitted Fundraising PHI can be used by or disclosed to a Business Associate or to a not-for-profit charitable foundation that is affiliated with a Covered Entity and has been formed, at least in part, for the purpose of supporting a Covered Entity and to raise funds for the Covered Entity's own benefit.

26. ***When sending an educational event mailer, may the outside of mailer identify a diagnosis as the topic of the educational event?***

In situations in which fundraising communications may occur at the event, best practice is to list General Department of Service on the outside of the mailer with specifics detailed within the inside of the mailer. A Covered Entity may also consider identifying any co-sponsor whose name may suggest a diagnosis, such as Juvenile Diabetes Research Foundation, inside the mailer.

27. ***Can a physician who specializes in the diagnosis and treatment of a specific disease or condition share PHI with a non-profit association that fundraises for research, awareness and treatment of diseases within that specialty?***

No.
The Covered Entity, including any member of its workforce, cannot use or share PHI with a non-affiliated, non-profit association for their fundraising purposes. PHI cannot be shared by a Covered Entity or any member of its workforce with a third party to be used for fundraising by the third party entity.

Discussion: HIPAA Privacy Requirements and Fundraising

Basic Rules about the Use and Disclosure of PHI for Fundraising Communications

The Final HIPAA Omnibus Rule (the "Final Rule") effective March 26, 2013 with compliance date of September 23, 2013 amended the elements that may be used in fundraising communications to allow for use of the following PHI without prior authorization from the patient, referred to as "Permitted Fundraising PHI":

1. Patient demographics including name, age, gender, date of birth, address, and contact information including phone number and email address;
   Where a Covered Entity targets pediatric patients, patient demographics are interpreted to include the parents and/or guarantors' demographic information.
2. Dates of service;
3. Department of service, i.e., information about general department of treatment, such as cardiology, oncology, that does not indicate a more specific type of diagnosis, nature of services or treatment received by the patient;
4. Treating physician name;
5. Outcome information, such as death or other sub-optimal results which may only be used to screen or exclude patient families from receiving fundraising communications; and,

6. Health insurance status, which is not defined in the Privacy Rule, but interpreted to mean whether patient is insured and type of insurance.

In order to use or disclose Permitted Fundraising PHI for fundraising communications, a Covered Entity must ensure that:

1. The Notice of Privacy Practices (NPP) contains a statement that a Covered Entity may contact the patient to raise funds and the patient has a right to opt-out of receiving fundraising communications;
2. Clear and conspicuous instructions are provided in all fundraising communications as to how the recipient can opt-out. The opt-out method must not cause an undue burden or cost to the patient; and
3. Processes are implemented to ensure it refrains from conditioning treatment or payment on a patient's choice regarding whether or not to receive fundraising communications.

Once these stipulations are met, a Covered Entity may use Permitted Fundraising PHI for fundraising communications without further authorization from the patient.

PHI requiring Authorization or Specific Consents (sensitive PHI)

Due to additional federal and applicable state privacy/confidentiality statutes and/or regulations that apply to certain types of services, a Covered Entity must consider potential additional restrictions to the use of Permitted Fundraising PHI related to such services, i.e., department of service, name of treating physician and date of service. It's important to note that many states statutorily restrict release of information related to Mental Illness or Developmental Disability, HIV/AIDS Testing or Treatment, Communicable Diseases, Sexually Transmitted Infections, Abuse of an Adult with a Disability, Sexual Assault, Child Abuse and Neglect, Genetic Testing, or Artificial Insemination without a valid consent signed by the patient in advance of use. Additionally, psychotherapy notes as defined under the Privacy Rule and certain substance abuse treatment information, including the fact that a patient received care, are protected under federal law [2] and require the explicit patient authorization/consent for most uses. These types of highly sensitive medical information should be excluded and made unavailable for any fundraising communication. A Covered Entity is advised to review the relevant state/federal statutes and regulations, determine whether applicable federal and state regulations are more restrictive and apply the more stringent standards to the Permitted Fundraising PHI prior to use or disclosure for fundraising communications**.**

"Opt-out" requirements must be clear and conspicuous and not impose an undue burden

A Covered Entity must provide "clear and conspicuous opportunity" to the patient to opt-out of future fundraising communications. If the patient opts out, it must be treated as a revocation of any prior authorization for use or disclosure of PHI for fundraising communications.
The method for a patient to opt-out must not impose an undue burden or more than a nominal cost on the patient. A Covered Entity should consider offering a toll-free number, an e-mail address, a web page, or similar opt-out mechanisms that are simple, quick and low or no cost to the patient. Requiring a patient to send a written letter opting out of fundraising communications would constitute an undue burden, although including a mailing a pre-printed, pre-paid, business reply postcard or directing a patient to an opt-out on a web page would be permitted.

[2] 42 CFR 2

A Covered Entity may permit general opt-out for all future communications, or to a particular fundraising campaign. Once implemented, however, a Covered Entity must not send such further fundraising communications. A Covered Entity may, at its discretion, allow patients to actively opt back in to receiving fundraising communications should the patient later change their mind.

Fundraising Opt-out Statement

The Final Rule does not provide specific wording for a Fundraising "Opt-out" statement. The following is provided as an example of a "clear and conspicuous opportunity" for patients to "opt-out" of any further fundraising communications.

If you do not want to receive future fundraising communications supporting [Insert Covered Entity's Name or fundraising campaign name], please check the box on the enclosed printed, pre-addressed and pre-paid card and return it by mail.

Alternatively, you can call [insert local number] or toll free [insert toll free number], email [insert email address] or fax [insert fax number] a message identifying yourself and stating that you do not want to receive fundraising requests. Or, simply tell us in person.

There is no requirement that you agree to accept fundraising communication from us, and we will honor your request not to receive any more fundraising communications after the date we receive your decision. Your treatment or payment will not be affected by your choice to opt-out of a fundraising communication.

Each Covered Entity must develop its own "opt-out" data management process based on available resources. The following are factors to consider in implementing "0pt out" of fundraising communications.

1. All fundraising communications to patients must include an "Opt-out" statement.
2. The "opt-out" process should be explained during solicitations made through one-on-one meetings, telephone conversations with donors, or in newsletters, brochures, invitations, emails, or letters.
3. A patient may communicate fundraising "opt-out" verbally by telephone or during an in-person conversation or in a variety of written methods including via email, mail, and fax, as instructed by a Covered Entity in its fundraising "Opt-out" statement.
4. A Covered Entity may determine if the "opt-out" will apply to all fundraising communications moving forward or to a specific fundraising campaign.

   If a Covered Entity chooses to limit opt-outs to a specific fundraising campaign, it must provide clear instruction to the patient of available opt-out choices. The patient's opt-out request must be accurately tracked and implemented by a Covered Entity. To implement opt-out choices as directed by the patient, a Covered Entity must have the capacity to track and adhere to such requests.

5. Once a request has been received, the Development staff must flag a patient's demographic information within the Development's database to ensure that future fundraising communication is not sent to the patient.
6. Non-Covered Entities' fundraising activities do not need to comply with opt-out requirements. For example, an alumnus may ask to be removed from all Covered Entity or patient fundraising efforts, but still receive university/alumni fundraising efforts.

A Covered Entity may accept a patient's revocation of a prior opt-out choice. A patient, however, must specifically revoke his/her prior opt-out decision. The patient sending a subsequent donation after opting out is not considered a revocation of the patient's opt-out. The Final Rule does not provide instructions for revocation of an opt-out, but best practice that is a Covered Entity creates a notice of revocation of opt-out form that the patient completes in writing and forwards to the Covered Entity to keep on file as documentation of the patient's request to opt back into receiving fundraising communications.

Notice of Privacy Practices "Opt-out" Statement

To use and disclose Permitted Fundraising PHI for fundraising communications, the Notice of Privacy Practices must include a statement that a Covered Entity may contact the patient to raise funds for the Covered Entity and the patient has a right to opt-out of receiving such communications. The following is offered as a sample statement only.

> *We may use certain information (name, address, telephone number or e-mail information, age, date of birth, gender, health insurance status, dates of service, department of service information, treating physician information or outcome information) to contact you for the purpose of raising money for [NAME OF INSTITUTION], but you have the right to opt-out of receiving such future communications [with each solicitation][3]. For the same purpose, we may provide your name to our institutionally related foundation. The money raised will be used to expand and improve the services and programs we provide to the community. You are free to opt-out of any or all fundraising solicitations and your decision will have no impact on your treatment or payment for services at [NAME OF INSTITUTION].*

Donors who may be Patients in the Hospital

When interacting with donors receiving care, the Development staff must follow the Covered Entity's privacy policies and the Final Rule. A Covered Entity may have staff visit patients who are donors as part of its patient-centric care. Visits by Patient and Guest Relations staff are considered part of patient care and/or customer services activities, i.e., Health Care Operations. These visiting staff would not make fundraising communications to patients, but may forward information to Development staff when a patient or other individual expresses interest in making a donation or speaking with Development. It is recommended that Development staff not initiate any visits with a new potential donor for fundraising communications while the patient is in the facility to receive health care services or while the patient is accompanying or visiting with a family member or friend who is receiving health care

[3] A Covered Entity may desire to add parenthetical phrase if a Covered Entity implements opt-out for each patient fundraising solicitation, rather than patient opt-out of all future fundraising communications.

services. A donor, as any patient, should not be visited if he/she have opted out of being published in the Facility Directory. During the course of receiving health care services, if a patient or patient's family member/friend expresses interest in making some sort of donation, or inquires about development activities to any staff, it is suggested that the staff member may obtain and share the patient's name and contact information with Development staff for follow-up. Generally such follow-up by Development staff occurs after the patient is discharged, unless the patient specifically requests otherwise.

If an existing donor specifically requests a visit from a Development staff member while the patient is receiving treatment in the facility,[4] it is suggested that Development staff consider:

- Any PHI acquired through incidental exposure during such a visit (e.g. learning the patient had foot surgery by seeing that the patient's foot is bandaged and elevated) should not be used for fundraising communications.
- If a donor requests assistance in coordinating clinical services, the Development staff should re-direct or introduce the donor to the applicable department or staff, such as introducing the donor to the Patient and Guest Relations program (which may be part of a Concierge or Special Constituency Program), and not intervene in the donor's clinical needs.
- Development staff may assist donors to schedule appointments by being a conduit to scheduling staff.
- If the Development staff accesses donors' PHI (more than Permitted Fundraising PHI) to assist donors, the staff must obtain the donor's signed authorization prior to accessing such PHI.

Fundraising Activities with Third Parties

Permitted Disclosure of PHI to Business Associate or Foundation for Fundraising Activity

A Covered Entity may disclose Permitted Fundraising PHI to a Business Associate or to an affiliated not-for-profit charitable foundation to raise funds for the Covered Entity's own benefit without first obtaining a patient's Authorization. The foundation must be affiliated with a Covered Entity and formed, at least in part, for the purpose of supporting the Covered Entity.

Third party vendors may be used to provide support services related to a Covered Entity's fundraising communications, e.g., mailing or database management. The Covered Entity should enter into a business associate agreement with the third party that specifies that the vendor will only use and disclose PHI to perform services on behalf of the Covered Entity and comply with the Covered Entity's vendor procedures, e.g., sanctions checks. The business associate is prohibited from using PHI for any purpose other than performing duties on behalf of the Covered Entity. The Covered Entity's employees and business associate's employees are prohibited from asking patients to execute a HIPAA authorization form to disclose PHI to permit a third party vendor to use information for its own purpose.

Educational Events Co-Sponsored with a Third Party

[4] If the patient requesting the visit is at the hospital to visit someone else who is a patient (e.g. husband who is an existing donor requests that a Development staff member visit while his wife is admitted), it is suggested that the visit should occur outside the patient room unless Development staff receives the patient's permission.

A Covered Entity may offer educational or awareness campaigns co-sponsored by a third party (e.g., American Heart Association) or include speakers or information from such third parties. A Covered Entity, however, is prohibited from sharing PHI with the third party or permitting the third party to use a Covered Entity's patient mailing list or Permitted Fundraising PHI to send co-sponsored fundraising solicitations. A Covered Entity should not include third party fundraising information within the event's communications, e.g., invitation, brochure or similar communication tools. At the event, the third party may invite patients to provide their contact information in writing, such as a sign up log, that clearly identifies the third party' request to contact the patients attending the event, including the possibility that they will be contacted for the third-party's own fundraising efforts. No fundraising related to the third party should occur at the event.

Combination of Permitted Fundraising PHI with Public Datasets

Permitted Fundraising PHI may be linked freely to available public datasets to refine the audience of a given fundraising campaign. For example, per capita income from publicly or commercially available datasets may be used to determine zip codes in order to target fundraising communications to patients who live in such zip codes that have higher disposable income. For example, a Covered Entity can identify grateful patients for a cancer center campaign by pairing data on patients who recently were treated in the oncology department with commercial or publicly available zip code data that identifies which residents have a higher per capita income. To target potential new gifts, a Covered Entity may screen patient names through a wealth capacity database.

Fundraising as a health care operation to support activities related to fundraising

The Final Rule is clear that only Permitted Fundraising PHI may be used or disclosed by a Covered Entity for fundraising communications. However, the Privacy Rule specifically includes fundraising in the definition of Health Care Operations, leading some Covered Entities to include its internal fundraising operations as part of its health care operations. These Covered Entities, as part of its health care operations, allow defined Development staff to use the minimum necessary PHI to perform internal operational activities. Such fundraising operational activities would not be considered fundraising communications.

A Covered Entity that uses PHI for its internal operational activities of the Development Department must be careful to distinguish the use of minimum necessary PHI for its internal operational activities from use and disclosure of Permitted Fundraising PHI for its fundraising communications. The Development staff needs to comply with the Privacy Rule's regulatory requirements for use and disclosure of PHI for health care operations rather than the requirements related to Permitted Fundraising PHI.

Under this interpretation, examples of such activities include providing reports to support event planning and prospect research. A Covered Entity that takes this approach should have controls in place to ensure that:

1. Only the minimum additional PHI data elements needed to perform fundraising operations activities are provided to Development staff. For example, patient diagnosis is not a data element needed or permitted by Development staff to perform health care operations activities.

2. Access to additional PHI by Development staff is restricted within the Development Department to those workforce members performing operations activities that support a Covered Entity's fundraising (to comply with minimum necessary and role-based access controls).
3. The reports produced as part of the fundraising operations activities and disseminated to Development staff contain only the PHI data elements that the Final Rule allows to be used and shared for fundraising communications (Permitted Fundraising PHI).
4. The Development Department has documented policies and procedures in place to explain the additional PHI elements needed to perform operations activities in the Department and the controls in place to limit access to the additional PHI handled by the Development Department for such activities.
5. Development staff receives routine and ongoing education on permissible and impermissible use and sharing of PHI for fundraising communications.
6. Fundraising communications are regularly reviewed to identify any compliance concerns by establishing regular dialogue between the Development Department, the compliance/privacy office and legal counsel.
7. Regular dialogue occurs between the Development Department, clinical departments and providers to coordinate and review fundraising communications to ensure compliance.

Definitions

Final HIPAA Omnibus Rule (the "Final Rule"): Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules. Final Rule published January 25, 2013 (Federal Register 78(17):5565-5702).

Business Associate: a person or entity that performs certain functions or activities on behalf of, or provides services to, a Covered Entity that involves the use or disclosure of PHI.

Covered Entity: health plans, health care clearinghouses, and health care providers that transmit health information electronically in connection with a HIPAA transaction.

Disclosure: release, transfer, provision of access to, or divulging in any manner of patiently identifiable health information outside a Covered Entity.

Protected Health Information (PHI): any information, whether oral or recorded in any form or medium that is created or received by a Covered Entity that identifies an patient or might reasonably be used to identify an patient and relates to:

- The patient's past, present or future physical or mental health; or
- The provision of health care to the patient; or
- The past, present or future payment for health care.

Information is deemed to identify a patient if it includes either the patient's name or any other information that taken together or used with other information, could enable someone to determine a patient's identity. For example: date of birth, medical record number, health plan beneficiary numbers, address, zip code, phone number, email address, fax number, IP address, license numbers, full face photographic images, or Social Security Number.

PHI excludes patient identifiable health information in education records covered by the Family Educational Right and Privacy Act (FERPA) (records described in 20 USC 1232g(a)(4)(B)(iv)) and employment records held by a Covered Entity in its role as employer. PHI also excludes health information of patients who have been deceased more than 50 years.
Use: Sharing, employment, application, utilization, examination, or analysis of such patient identifiable health information within a Covered Entity

Permitted Fundraising PHI:

1. Patient demographics including name, address, contact information including phone number and email address, age, gender and date of birth;
2. Dates of service;
3. Department of service (meaning information about general department of treatment such as cardiology, oncology that do not indicate a more specific type of diagnosis, nature of services or treatment received by the patient);
4. Treating physician name;
5. Outcome information (such as death or other sub-optimal results and may only be used to screen or exclude patient families from receiving fundraising communications) ; and,
6. Health insurance status (not defined in the Privacy Rule, but interpreted to mean whether patient is insured and type of insurance).

Fundraising Communication: A communication to a patient that is made by a Covered Entity, an institutionally related foundation, or a business associate on behalf of a Covered Entity for the purpose of raising funds for the Covered Entity. The definition includes appeals for money and sponsorship of events, etc., but does not include royalties or remittances for the sale of products to third parties with the exception of auctions or rummage sales, etc.