TIP SHEET

6 Tips to Navigate HIPAA and PHI in Your Healthcare Fundraising Organization

BY MARTI ARVIN, Executive Advisor at CynergisTek, Inc.

The use and disclosure of protected health information (PHI) for fundraising can be quite complex and it is crucial for the development team to effectively navigate the regulations, relationships, and compliance so they are able to help patients express gratitude through financial gifts.

1 Know what internal teams need.

In order to do as much outreach as possible to the best patient prospects, the development team needs to be able to effectively communicate within the hospital or health system. Be prepared to have conversations with these groups and answer questions about how you are using and storing the data provided. This includes understanding the capabilities and security of your fundraising technology.

Compliance/Privacy Officer

- Most interested in ensuring information about patients is only shared in a compliant manner under HIPAA and other applicable laws.
- Responsible for ensuring information sharing follows applicable state and federal laws and organizational policies. For example, state law may go beyond HIPAA in restricting the sharing of some types of information, such as genetic information. If sharing a patient's department of care would, in effect disclose this information, the compliance officer may object to it being used for fundraising.
- Ideally, the compliance officer will work to balance the desire to increase funding for mission critical functions, such as improved care and research, with the goal of protecting patient privacy.

Information Security Officer

- Responsible for ensuring the technology infrastructure of the organization is secure, that any application allowed to connect to that infrastructure does not introduce unwarranted risk to the environment, and any connection used for the sharing of information is secure.

- Establishing policies and procedures around data governance to be followed by everyone in the organization.
- Assessing and implementing system controls around patient information.

Senior Leadership Team

- Fostering collaboration between the development team, compliance officer, and information security officer to ensure PHI is protected.
- Making a final decision on the balance between raising money and meeting legal obligation and minimizing risks.

2 Know the regulations.

It is the development team's responsibility to understand organizational, state, and federal regulations related to information sharing for fundraising purposes. When in doubt, ask the appropriate person within your organization.

According to the HIPAA regulations (revised in 2013), the following information is explicitly listed as sharable with hospital fundraisers without the individual's authorization:

- Name
- Address and other contact information
- Age
- Gender
- Date of birth
- Department of service
- Treating physician
- Outcome information
- Insurance status

Where a term is not explicitly defined in the regulations, best practice is for the covered entity to create a policy defining its interpretation of the term. For example, do email addresses and phone numbers constitute "other contact information?" Thoughtful consideration of issues like these make it easier for your team to understand what can be requested for fundraising.

Ensuring compliance beyond just HIPAA regulations reinforces the importance of continued dialog with the compliance/privacy officer and information security officer. Make sure any new data set requests go through the proper channels so each team can confirm compliance. This reduces liability for the organization which would only be exacerbated if a data compromise were to occur.

3 Know who you can share with.

According to the revised HIPAA regulations (in 2013), patient-authorized information can be used internally, shared with a business associate for fundraising, and disclosed to an institutionally related foundation.

To ensure patient authorization for PHI to be used in fundraising, the covered entity must include a provision in its notice of privacy practice (NPP) that allows limited information for fundraising. If the covered entity has not included such a statement, then any use of PHI for fundraising must have the patient's authorization. In addition to the NPP, including notification of the uses and disclosures of PHI for fundraising, the entity must also inform the patient of the right to opt-out of having their PHI used for fundraising. The opt-out information must also be included in any solicitation for fundraising.

4 Understand your relationship to the covered entity.

This is important to understand because the obligations to protect the information and the breach notification laws applicable to the information may vary based on this relationship. If the development team has signed a Business Associate Agreement (BAA), the development staff is covered by HIPAA regardless of their relationship to the covered entity.

Individually identifiable health information (IIHI) is PHI if

- It is held by the covered entity
- It is held by the covered component of a hybrid entity
- Shared with a business associate supporting the covered entity's fundraising efforts

It is not PHI if

- The information is in the possession of an institutionally related foundation
- The foundation receives IIHI from a donor and subsequently shares it with a vendor supporting fundraising efforts

5 Implement good data governance standards.

Best practice for organizations, regardless of their need to comply with HIPAA, is to follow fair information practices, which means only collecting the information needed, using it for the purposes for which it was collected, and only retaining if for as long as it is needed.

The development staff should think beyond "can we get the data" to "should we get the data." Identify a defined need for each data element requested from the covered entity. This helps keep the data to the minimum necessary.

It may be helpful to ask yourself questions as you consider requests. If the patient is a minor, do you need the minor's information or could you only request the parent/guardian/guarantor?

If a wealth screening has been conducted and a conclusion reached that no further action will be taken to target a certain segment of those screened, is it necessary to continue to hold the information? Once a wealth screening has been performed and the individual's information has been transferred to the prospect tracking system, can and should duplicate data be eliminated from the wealth screening system?

Work with the compliance/privacy officer and information security officer to create strong policies and procedures regarding these types of questions. Minimizing data in your possession can also minimize the impact of any data compromise: data that is not there cannot be compromised.

6

Store PHI appropriately.

This often falls under the purview of the information security officer for the covered entity, but it is important the development team understands the organization's approach.

It is important to remember that encryption is not a panacea. If a development employee leaves their username and password in a place where it can be compromised, any protection from encryption could be lost, even if the server is fully encrypted.

Multi-factor authentication is a tool that provides protection, as long as it is used. If possible, choose fundraising software that integrates with the organization's authentication method.

Learn more in *HIPAA and Fundraising: Understanding the Regulations, Roles, and Compliance.*

Download Now

DISCLIAMIER: All the opinions in this article are the author's own and don't reflect the opinions of Blackbaud. Further, nothing in this article is intended to be legal advice—please consult your organization's own legal counsel.

About Blackbaud

Leading uniquely at the intersection point of technology and social good, Blackbaud connects and empowers organizations to increase their impact through cloud software, services, expertise, and data intelligence. We serve the entire social good community, which includes nonprofits, foundations, companies, education institutions, healthcare organizations, and the individual change agents who support them.