HIPAA and Fundraising: Understanding the Regulations, Roles, and Compliance

BY MARTI ARVIN, EXECUTIVE ADVISOR, CYNERGISTEK, INC.

The use and disclosure of protected health information (PHI) for fundraising may seem straightforward but can be quite complex. Three factors in particular make it less straightforward.

1. *Understanding the regulations.*
2. *Understanding the organizational structure and relationship between the entity or entities involved.*
3. *Understanding what data to collect and how to be a good steward of the information.*

The outcome that achieves everyone's goal can vary by organization and the risk tolerance of the organization as a whole. It also varies with the influence and sophistication level of each constituent. If a conversation is occurring with the development officer, it should not be assumed that individual has been working with the compliance/privacy officer. There may also be known and unknown pressures for any of the key players to "make it happen." The needed understanding of the rules and the relationship of the parties may not always be present in the organization. Understanding what the regulations permit and do not permit is a good starting point.

Contents

This white paper is for informational purposes only. Blackbaud makes no warranties, expressed or implied. 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.

Understanding the Regulations

What can be shared

Under the original HIPAA regulations, there was not explicit regulatory language addressing what information could be shared for fundraising, forcing organizations to make determinations on their own, which could have negatively impacted fundraising.

The regulations only identified demographic information and the dates health care was provided as the information that could be shared for fundraising.i The preamble provided some additional clarity on what the Department of Health and Human Services (DHHS) was thinking regarding demographic information, but it was still not explicit. For example, it included contact information but did not provide guidance on the specific data elements that would be considered contact information. It did explicitly state that information regarding illness or treatment could not be shared.[ii]

While this permitted the use and disclosure of PHI for fundraising, the limited information and lack of regulatory clarity on exactly what demographic information included left some doubt. Healthcare organizations were left on their own to determine how comfortable they were with encompassing information under this term.

When the HIPAA regulations were revised in 2013, the DHHS Office for Civil Rights (OCR) shifted definitions from the preamble to the actual regulations. This change to the regulations provided additional clarity regarding what healthcare organizations were permitted to share. However, the minimum necessary was expected to be considered when sharing information for fundraising.

The following information is now explicitly listed as sharable with healthcare fundraisers without the individual's authorization:

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

Where a term is not explicitly defined in the regulations, it is best practice for the organization to have a policy defining its interpretation of the term. For example, insurance status is a data element that can be shared for fundraising, but what does that mean? Is it whether the patient has insurance, a yes or no question? Is it the type of insurance the patient has i.e., none, commercial, Medicare, Medicaid, etc. There is nothing in the preamble to the rule clarifying this.

Similarly, the regulations do not define other contact information. In order to determine what information can be shared for fundraising, best practice is for the covered entity to determine what it believes constitutes “other contact information,” for example, email address and phone numbers. For purposes of what a covered entity would allow to be used for fundraising, they may consider whether it would be just home phone, home and cell, or home, cell, and work phone, if a patient has provided all three. Thoughtful consideration of issues like these makes it easier for the development staff to understand what can be requested for fundraising.

With Whom the Information Can Be Shared

Another provision to the regulations was that the information could be used internally or shared with a business associate for fundraising. Organizations were also permitted to disclose information to an institutionally related foundation. An institutionally related foundation is not defined in the regulations, however the preamble to the 2000 final rule made it clear that there must be a direct relationship between the foundation’s mission and the covered entity. We will explore this relationship in the next chapter, but it is clear that sharing PHI in any other way or with another party such as a disease-related fundraising organization or nonprofit would require an authorization from the patient.

Notice of Privacy Practices

For any PHI to be shared for fundraising without patient authorization, the covered entity must include a provision in its notice of privacy practice (NPP) informing the patient that it may use 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.

Understanding Organizational Roles and Structure

Understanding the roles within the organization is important. Being prepared to discuss the concerns of the compliance/privacy officer and/or the information security officer is critical to helping obtain the appropriate information for fundraising. Successful fundraising is a team sport. The more all parties involved can understand each other's role and perspective, the increased ability to do it well while minimizing risk to the organization.

COMPLIANCE/PRIVACY OFFICER

The compliance/privacy officer is often concerned about sharing some information based on provisions of state and federal laws and organizational policies. For example, state law may further restrict the sharing of some types of information, such as sexually transmitted infections or genetic information. If sharing a patient's department of care would, in effect disclose this information, the compliance/privacy officer may object to it being used for fundraising.

As a former compliance/privacy officer at four different academic medical centers, my view on what information can be shared for fundraising was focused on not only what can be legally shared but whether the organization should be sharing the information. Ideally, I tried 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

The information security officer often looks at the method for transmitting and storing the information. There may not be as heavy a focus on the exact nature of the information being shared. The focus will be on factors such as whether the information is encrypted and other system controls around the information.

If the request for information comes from the development officer to the information technology (IT) team, there may be an assumption the appropriate approvals have been obtained. It could also be the IT team does not know what can be shared for fundraising or that the information being requested is beyond the minimum necessary. It's important to remember their primary interest is the security of the information.

If information *can* legally be shared, that does not mean it *should* be shared.

DEVELOPMENT TEAM

The development team wants to provide the maximum opportunity for giving to the organization by identifying the individuals with not only the capacity, but also interest in donating to the organization. This team looks at the goal from many angles, including reviewing individual donors who can provide large gifts, annual campaigns sent to larger groups who might provide smaller donations that, in the aggregate, result in a significant contribution, and the individual or smaller group of donors who may be interested in supporting a particular cause such as research for a particular disease or a new diseased focused treatment unit.

All the projects require data, but the amount for each will likely vary. Best practices for the development team include:

- Taking a ”big picture” approach to data requests.
- Having conversations with the compliance/privacy officer about what data is needed and for what purpose.
- Evaluating the data fields you actually need to accomplish the intended goal. This best practice reflects the Minimum Necessary Requirement in the HIPAA Privacy Rule, which is a protection requiring covered entities to limit unnecessary disclosure of PHI to carry out a particular purpose.
- Being familiar with the fundraising system capabilities and the security controls of the locations where data is stored and the technology solutions they use.

No one should expect the development team to be experts in these areas, but it is important to know enough to answer basic questions and to direct their compliance colleagues in privacy and information security to the right people for the more detailed discussion. This may sometimes even necessitate helping the development team better understand the rules for fundraising and sharing PHI. It may also be necessary to remind them to consider factors such as minimum necessary.

SENIOR LEADERSHIP

Best practice says the risk tolerance for the organization is always a decision for senior leadership. Compliance/privacy officers do not always recognize that the level of risk tolerance they are comfortable with may not match the level of risk tolerance their organization is comfortable with in a particular circumstance. Compliance/privacy officers may prefer no information is shared with a business associate or institutionally related foundation for fundraising. However, the senior leadership may be comfortable with sharing the information, as permitted by HIPAA and other laws. Often, making recommendations on how to reduce the risk is the role of the compliance/privacy officer, and the chief information security officer, but the ultimate decision rests with senior leadership.

Organizational Structure

Another key fact is understanding the organizational structure of the healthcare entity conducting the fundraising activity and the relationship to other entities involved. The development staff may be employed by the covered entity or the institutionally related foundation of the covered entity. If the covered entity is a hybrid entity, the development staff employed by the hybrid entity must be inside the healthcare component if they wish to have access to PHI for fundraising without an authorization.

These relationships are important to note because the nature of the information may vary depending on whose hands it is in. If the covered entity engages a third-party to support its fundraising activities, that relationship would require a Business Associate Agreement (BAA). The data shared with the business associate entity would maintain the PHI designation and still be covered by HIPAA.

If the individually identifiable health information (IIHI) is in the hands of the covered entity or the healthcare component of a hybrid entity, it is PHI. If it is in the possession of an institutionally related foundation, it is not likely PHI.

If the development staff are part of the covered entity or inside the healthcare component of a hybrid entity, any IIHI they collect would be PHI. This could include information collected from a potential donor even if that person was not a patient of the organization. The definition of PHI does not distinguish between the IIHI a covered entity collects from a patient versus from someone else. If the data fits the HIPAA definition of IIHI and it is maintained by a covered entity, it is PHI. This is important to understand because the obligations to protect the information and the breach notification laws applicable to the information may vary.

The same would be true if the information is shared with an institutionally related foundation. An institutionally related foundation is not likely a covered entity under HIPAA. Thus, if the foundation receives information and subsequently shares it with a vendor, the information is not PHI. This means it is not subject to the breach notification provisions of HIPAA. However, it may be subject to the breach notification obligations under other laws.

As a best practice, organizations, regardless of their need to comply with HIPAA, should 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.

Understanding the perspectives of the various parties involved and the organizational structure is important to understanding the legal obligations around protecting information. It is also important to understanding the risk reduction controls the different players may choose to implement within an organization. This is not one size fits all.

Understanding Good Data Governance

It is important for the development team to remember that the compliance/privacy officer and Information security officer share the goal of doing what is best for the organization, but their priorities are not the same as development and they likely see risk differently. The more the development staff can understand and prepare to be responsive to their concerns, the smoother the process will go. This will also likely reduce the overall risk to the organization.

What Data is Actually Needed to Accomplish the Fundraising Goal?

The first consideration, what data is needed to accomplish the fundraising goal, is an important one and requires discussions with the development team. Sharing all PHI permitted under the law is not always necessary and when unneeded information is shared, it can become a liability for the organization. By working together, the development and compliance teams can determine the right balance in the amount of data shared by the covered entity.

For example, if a wealth screening is being performed, should the information for all patients be shared? Only if the organization is screening all patients. If the organization does not plan to do a wealth screening on patients under the age of 25, then information on these patients does not need to be given to the development team.

However, for a children's hospital, sharing information on most patients may be necessary to be able to conduct a wealth screening on the parents of certain patients as the potential target of a fundraising solicitation. This is another instance where the healthcare organization will need to make a decision. The regulations do not specify that a parent or guarantor's name can be used for fundraising. Can this be considered "other contact information"? Organizations might consider defining this in an institutaional policy. When the solicitation is focused on pediatric patients, the development team should consider issues such as if the parent or guarantor's name is shared, is the patient's name necessary? If it is initially needed, does any other patient specific information need to be to be retained?

The development staff needs to think beyond "can we get the data" to "should we get the data." There should be a defined need for each data element requested. This helps keep the data to the minimum necessary and may have an impact on the analysis should a data compromise occur.

DATA GOVERNANCE

Take advantage of technology! By automating data transmission between the covered entity and fundraising organization, you can set very specific parameters around the data that is shared, reducing liability.

- Exclude information on minor patients, if appropriate.
- Exclude based on characteristics that make patients unlikely to give (zip code or insurance status).

The compliance/privacy officer may be asking these questions of the development staff, but even if this is not happening, the development staff should be thinking about minimum necessary and only requesting the information actually needed to meet the goal.

Where is the Data Being Stored?

The information security officer and compliance/privacy officer will be interested in understanding the fundraising organization's data storage plans. There may be data elements that have served an intended purpose and no longer need to be retained. 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?

If it is determined that individually identifiable information, including PHI, should be retained, is it necessary to retain all the information? Good data governance, beyond the HIPAA regulations, warrants that organizations ask themselves these questions. An acronym used by data managers is ROT, which stands for redundant, obsolete, and trivial. Good data stewards will always be considering this and ensuring any data set they maintain does not have any ROT data.

For example, if an individual has been contacted and made it clear they are not interested in making a donation, is it necessary to keep all of their contact information? Can data elements like the date-of-birth, treating provider, insurance status, or service department be deleted? Another consideration when thinking about ROT is to determine if the same data needs to be retained in multiple locations. 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?

The organization's analysis should determine the minimum data set to retain as a record and the storage location. This will require a coordinated thoughtful effort and structured processes between the compliance/privacy officer, information security officer, and development officer. Ensuring there is not ROT data helps minimize the impact of any data compromise: data that is not there cannot be compromised.

In addition to organizational policies, all parties involved should be considering any state or federal law provisions for retaining information. When a data compromise occurs and individuals are notified their information might have been involved, a legitimate and common question is, "why did you have my information?" This will be even more likely when the information was in the hands of a business associate or an institutionally related foundation. The legal liability to the organization may be increased if the information was retained longer than necessary particularly if the retention was inconsistent with the organization's policies.

For example, some organizations may allow development staff to visit prospective donors while they are inpatients. Providing the development team with the patient's room number may be necessary for this purpose, however, is there any need to retain the information once the individual has been discharged or it becomes clear there is no likelihood of a donation?

In What Format is Data Being Stored?

The format of data storage is also an important factor. The information security officer for the organization will most likely be looking at this consideration, but it could be the compliance/privacy officer as well. It is important to note that encryption is not a panacea. End users remain one of the biggest risks to data. If a server is fully encrypted but a user leaves their username and password in a place where it can be compromised, any protection from encryption could be lost. Organizations should have policies and procedures in place regarding the expectations for end users. There should also be good training and education so that individuals understand their role and obligations in data protection.

Another consideration is whether a system requires a single method of authentication or multi-factor authentication. When considering authentication method used by a technology tool to support activities such as fundraising, one factor may be considering how easily the tool integrates with the organization's processes. Ideally, the tool would integrate with the organization's authentication method, but this may not always be feasible. Organizations will need to weigh the importance of this against the risk to the data.

Are There Regulations Beyond HIPAA to Consider?

If an organization is subject to the Substance Abuse and Mental Health Services Act (SAMSHA) regulations, there are additional protections regarding how SAMSHA information can be shared. There may also be state laws regarding how specific information can be used and disclosed. These may include genetic, behavioral health, and/or sexually transmitted infections. When thinking about what information may be shared for fundraising, everyone should keep this in mind. If the organization is trying to raise money to support its substance use disorder (SUD) program, simply complying with HIPAA when considering the data to share may not be enough. That data may be protected by SAMSHA regulations and thus require explicit permission before any information can be shared with the development team.

This is why continued dialog with the compliance/privacy officer and information security officer is extremely important. If the development staff asks for a new data set that could encompass this type of information, it will be important to ensure the request has gone through the proper channels. If the data is shared in a non-compliant manner, this creates liability for the organization which would only be exacerbated if a data compromise were to occur.

Conclusion

Successful fundraising for any healthcare organization requires a thoughtful, collaborative effort among a number of stakeholders. The various parties involved will bring different viewpoints into the mix. Take advantage of the collective expertise. Everyone needs to understand what can be done under the various laws and regulations and the relationship of the entities involved. Being vigilant data stewards will also support the organization's efforts. Following this course means the goal to gain as much support as possible for the missions of the organization while minimizing risk can be accomplished.

About the Author

Marti Arvin brings more than three decades of operational and executive leadership experience in the fields of compliance, privacy, information security, research and regulatory oversight in academic medical and traditional hospital care settings to her position in CynergisTek. Arvin leads strategic business development around compliance services and utilizes her industry recognized expertise in healthcare compliance to inform the development of compliance, privacy, and security services to meet healthcare's under served needs. She is a nationally recognized speaker and contributor to the thought leadership around healthcare compliance, privacy, information security, and research, and contributes to CynergisTek's industry outreach and educational programs. Arvin has extensive experience in building and managing compliance and programs for large academic medical centers.

Arvin previously has held the roles of Chief Compliance Officer and/or Chief Privacy Officer for Regional Care Hospital Partners, the UCLA Health System and David Geffen School of Medicine, the University of Louisville, the University of Pittsburgh Physicians, and the Indiana University School of Medicine. She has a legal background from obtaining her J.D. and holds CHC-F, CCEP-F, CHRC and the CHPC certifications. She is recognized as an expert on compliance and privacy issues from her published articles, lectures and presentations at national conferences. She was a board member to the Health Care Compliance Association between 2008 and 2011 and was on the Compliance Certification Advisory Board for over eight years. She also served on the certification committee for the CHC, CHC-F, CCEP, CCEP-F, CHRC and CHPC.

i 45 C.F.R. § 164.514(f)(1)
ii 65 Federal Register p 82719 December 28, 2000.
iii 45 C.F.R. § 164.514(f)(1)(i)
iv 45 C.F.R. § 164.514(f)(1)(iii)-(v)
v 65 Federal Register p 82546, December 28, 2000

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.