

The Ethical Considerations of Prospect Research and Relationship Management in Healthcare

David Lamb, Senior Consultant, Target Analytics, a Blackbaud Company

Executive Summary

Stories in the media shed light on the disconnect that exists between the legitimate needs of a healthcare institution to raise funds to pay for equipment, salaries, and services on the one hand, and the expectation of complete privacy in the healthcare context on the other. Should everyone expect complete privacy in a healthcare setting? Healthcare institutions have a practical need for support and have realized more in recent times that private support from philanthropic donors has become an essential source of funding for the medical enterprise. Grateful patients are the bedrock of many fundraising programs in healthcare. This paper focuses on some of the unique challenges of fundraising in a restricted environment.

Excerpts From News Headlines And Stories

Law Allows Hospitals to Use Patient Records for Fundraising¹

When Steve Finn got a call on his unlisted telephone number from the University of Washington Medical Center seeking a donation, he was perplexed. How on earth did the caller get his name and number?

Finn, a 62-year-old retired CPA who lives on Queen Anne Hill, a one-time patient at the UW, knew that a broad federal law known as HIPAA protects patient privacy. So he was astounded when the caller told him the information had come from patient records.

It seemed logical to Finn that the law, which bars patient information from being used for commercial purposes, would also bar its use for fundraising. He also wanted to know: What did the caller know about him? Was the caller a "qualified health professional" entitled to his information under the law? And how could he get off the list?

In fact, HIPAA specifically allows medical centers to use patient information for fundraising activities, explained Richard Meeks, director of the UW's privacy program.

Finn said he was disturbed because HIPAA bars using patient information for commercial purposes.

Contents

Executive Summary	1
Excerpts From News Headlines And Stories	1
Introduction	2
HIPAA.....	4
Confidentiality	5
Electronic Security	6
Data Management.....	7
Research and Reporting	7
Back to Basics	8

Continued on following page

“Excuse me, but raising millions of dollars to support UW — a commercial enterprise hiding behind a not-for-profit mask — certainly sounds like a bending of the rules to suit a purpose,” he said. “You just feel as though your privacy is being violated. ... Just because HIPAA might allow UW to do this does not make it right.”

Hospitals, Patients Clash on Privacy Rights²

Joan Broner, like many people, never reads the fine print at her medical appointments. As a consequence, the 58-year-old San Francisco resident, who has arthritis, regularly receives solicitation letters at home from several local hospitals. The letters infuriate her.

“It feels like an invasion of privacy,” she said. “If I’m sick and I go to a doctor, I don’t want them telling anybody about it. My disease is not for sale.”

When patients check into hospitals or doctor offices, they presume their information will be kept in strictest confidence, but often, amid the pile of papers, they overlook fine print describing how their personal information can be farmed out for fundraising.

Hospitals and other health care organizations widely use patient information, without patients’ explicit permission, to raise funds. To the dismay of privacy-rights advocates and some in the medical field, fundraising to benefit medical institutions is allowed under federal law.

Fundraising efforts by UCSF led to a recent privacy breach involving more than 6,300 patients whose names and other information were inadvertently posted on the Internet — the institution had shared patient information with a vendor that searches databases to find wealthy potential donors.

Introduction

The stories from these newspapers and other similar instances that occur around the country shed light on the disconnect that exists between the legitimate needs of a healthcare institution to raise funds to pay for equipment, salaries, and services on the one hand, and the expectation of complete privacy in the healthcare context on the other.

It is ironic, in a way, that anyone should expect privacy in a healthcare setting. Having been a patient myself, it always seems to me that personal space is in very short supply at a hospital. For starters, wearing a hospital gown and having different people come into your room at all hours can be a bit invasive and humbling.

However, the central issue about healthcare privacy is not about the personal indignities of medical attentions, but how the public release of information about your health might impact other areas of your life. Medical care addresses the body and the mind, and these are subjects about ourselves that most of us prefer to have some control over, especially when it comes to when, where, and to whom they are revealed.



About the Author

David Lamb joined Blackbaud in 2004 following three years as an independent consultant for prospect research. David has more than 20 years of experience in the prospect research field. His Prospect Research Page (www.lambresearch.com) is a trusted and popular resource among prospect researchers. David is a frequent speaker at professional conferences, including those sponsored by the Council for Advancement and Support of Education (CASE), The Association of Fundraising Professionals (AFP), and The Association of Professional Researchers for Advancement (APRA). His areas of expertise include prospect research, prospect management, fundraising, and database systems. In 1997, he received APRA’s Service Award for outstanding service to the profession, and in 2001, he was awarded the CASE Steuben Apple Award for excellence in teaching. He holds a bachelor’s degree in sociology from Sterling College (Sterling, Kansas), a master’s degree in sociology from Wichita State University, and a Master’s in Divinity from San Francisco Theological Seminary. You can contact David at David.Lamb@blackbaud.com.

Continued on following page

The disconnect that I referred to earlier gets at the very core of the concept of the doctor-patient relationship. There is a cultural expectation that this is a privileged relationship, much like the confessional in a church. The exchanges between a health professional and a patient are considered sacrosanct. It is a matter of trust. Many — perhaps most — patients extend that expectation of confidentiality to the entire healthcare enterprise. Any revelation that seems to breach that trust tears at a social norm that most people take for granted. And for some, even the revelation that a person was ever a patient is considered such a breach.

Yet, healthcare institutions have a practical need for support. Years ago it was assumed that the fees paid by patients and support from government agencies supplied all the needs of the physicians, caregivers, and the infrastructure they used to treat patients. If that was ever true, the healthcare community has realized in recent times that these sources are no longer enough to meet the needs of modern medicine. Private support from philanthropic donors has become an essential source of funding for the medical enterprise.

The tension between the financial needs of medical institutions and the patients' expectation of privacy is heightened by a parallel controversy over the skyrocketing cost of drugs, medical equipment, and treatment. In the mix is a raging debate over the cost of health insurance. So when we hear complaints like the ones in the referenced newspaper clips, it's not 100 percent clear that people are upset about only one aspect of their relationships with their care providers.

As a result, we have huge misgivings about medical care as a culture. We want the best medicine, we want it inexpensively, and we don't want anyone to know we got it. It turns out that none of these values coexist comfortably with each other.

Let's acknowledge that we can't solve all of these problems. As fundraisers, though, we play an important role in addressing the cost issue. In order to do our jobs, we cannot avoid the privacy issue.

Medical care is generally thought to be a common social good much like education. Both institutions, education and medicine, are often supported by community leaders because education and medicine both make the society stronger. These generous benefactors provide essential resources that improve the quality of the services. But these donors, whose only motive is altruism, are often few in number. The hospital or the university must have broader bases of support. So they turn to their unique, built-in constituencies. Educational institutions have alumni; medical facilities have patients.

As we have seen by the negative press, though, many patients prefer to go "incognito." But many others are grateful for the care they received, just as alumni are grateful for their education. These grateful patients are the bedrock of most fundraising programs in healthcare.

Continued on following page

HIPAA

Since 1996, the Health Insurance Portability and Accountability Act (HIPAA) has described the boundaries within which fundraising from patients can operate. The law defines a concept called Protected Health Information (PHI). This includes:

- Name & Address
- Nature of treatment & Department where treatment is received
- Dates
 - Birth and death date
 - Admission and Discharge date
- Phone & fax numbers
- Email address & URLs
- SSN
- Health insurance information
- Account numbers
- Vehicle identifiers
- Biometric information
- Photos that identify the individual
- Any other unique identifying information

A patient's authorization must be obtained before any of the above information is disclosed for any purpose, with the following exceptions:

- Treatment
- Payment for treatment
- Some administrative operations (including fundraising)
- Other disclosures as required by law or compelling public purpose

The PHI that can be disclosed under these exceptions is limited to the minimum necessary to accomplish the specific task. For fundraising, the minimum information has been defined as:

- Demographic information
 - Name, Address, Age, Gender
 - Other contact information (phone number, for instance)
- Dates of service
- Insurance status

Continued on following page

Specifically excluded from use for fundraising — unless authorized by the patient — is information about a patient's illness, treatment, or services provided.

This last prohibition has been particularly galling to healthcare fundraisers. The comparison to educational fundraising again is apt. When administrators at a school of engineering want to build a new nuclear reactor, they naturally contact their alumni — former students who are grateful for their education and who understand the value that the new equipment will bring to the school and its students. When professionals in the oncology department at the hospital want to purchase a new piece of high-tech diagnostic equipment, they want to turn to their “alumni” — former cancer patients who are much more likely to be sensitive to the needs of fellow cancer patients than, say, former maternity or cardiology patients.

Since they are prohibited from using treatment or department information in solicitations, fundraisers are forced to be less targeted in their appeals, sending materials to a larger audience to reach the subset of the audience who is most likely to respond.

In addition to these restrictions on patient information used for fundraising, HIPAA further requires that the patient be given the opportunity to opt-out of future fundraising appeals after they are contacted for the first time. In the news story about the unhappy University of Washington Medical Center patient, the newspaper reported that 150 of the 6,000 patients who were solicited in the previous year opted out. That's 2.5 percent.

In the early days of HIPAA, some medical centers allowed patients to opt-out at check-in. Under those circumstances, 20 – 30 percent typically did so. So it has become the industry practice to stick to the letter of the law that only requires the opt-out option after the fundraising fact.

All of these restrictions, and other aspects of their healthcare privacy protection, are outlined for patients in a document called a Notice of Privacy Practices. Anyone who has so much as visited the doctor since 1993 has received this thick pamphlet upon admission and have been asked to sign a form acknowledging receipt.

With this background, I'd like to frame the ethical issues regarding healthcare fundraising around four topics:

- Confidentiality
- Electronic Security
- Data Management
- Research and Reporting

Confidentiality

APRA has had sessions on privacy and ethics every year for at least the last 15 years. The entire fundraising industry is sensitive to the issue of confidentiality. If everyone agrees that privacy and confidentiality is important, what makes healthcare special?

Continued on following page

We have to recognize that sometimes disease carries a stigma. No matter what one's personal belief may be about the value-neutrality of illness, some people are ashamed or embarrassed to be sick. If a person is receiving treatment for addiction or depression, they may be rightly concerned that some people will judge them harshly.

HIPAA is silent on what responsibilities a fundraiser has when information is obtained through means other than patient records. After a relationship has been established with a donor, the individual may self disclose information that, had it come from patient records, would have been protected. This is where ordinary professional ethics must kick in.

Early in my prospect research career, I was profiling a person who had been treated for breast cancer. This information was included in a contact report. My supervisor discussed this with me after reading the profile. At the time I was working for a university without a medical center. We decided that the nature of the medical treatment was not important in this context. It was sufficient to say in the profile that the prospect had been seriously ill and was still in the process of recovery.

This was before HIPAA, and the use of the information would not be strictly prohibited by HIPAA even now because it was not obtained through patient records. But the spirit of HIPAA was at play here. And that same spirit should govern all prospect research and fundraising activity. The minimum level of information required to accomplish the fundraising goal should be included in the prospect's record.

Electronic Security

The electronic security of medical information has become a news item recently with the Obama administration's initiative to put every person's medical records online by 2014. Making medical information easily transferrable like this can make healthcare processes more efficient and informed. It can also make it more vulnerable to inappropriate disclosure.

From a fundraising standpoint, horror stories like the one involving UCSF Medical Center give one pause. An electronic screening vendor accidentally stored patient names on a server that was open to a web crawler. This is not the only case where a vendor has been implicated in unintentionally leaking private information about a nonprofit constituency.

There are two issues that are in play here. One is technological, the other deals with information handling policy. On the technological side, extraordinary measures should be taken to make sure that donor information (and this applies to all donors and prospects, not just patients) is not accessible via a public web server. In the increasingly interconnected world of electronic information exchange, it is probably not possible or desirable to completely disengage patient information from the Internet. However, it is imperative that firewalls and passwords and other appropriate security measures be put in place to ensure that personal information is only accessible to authorized people.

Continued on following page

One researcher told me that her IT department would not allow transfer of patient data to a screening vendor via FTP. You can see how this can put a kink in a process of daily or weekly patient screenings. We should look for compromises that do not excessively tie the hands of the fundraisers but still protect patient privacy.

The policy issue involves rules that should be put in place to keep people from circumventing the technological issues. Ongoing education of staff members will remind everyone of what data are protected and how they should be handled. Vendors must provide assurances that they will enforce the same safeguards or pay a serious penalty. Leaks will still happen because humans are fallible, but this is a matter that deserves constant vigilance.

Note that, for screening purposes, vendors do not need any information that is not allowed by HIPAA. The law does allow for this information to be disclosed to “business associates” of the healthcare provider. So it is not the permissibility of the information that is in question, but rather its security.

Data Management

Despite the fact that all healthcare institutions must comply with the same law, there is considerable variation from one institution to another as to the level of access that the development department has to patient data. HIPAA compliance officers at different institutions interpret and apply the law differently. It can be very helpful to have a good face-to-face relationship with your HIPAA compliance officer. As much as the patient needs to trust the healthcare institution, an internal level of trust must be built with the gatekeepers of patient data. There are several levels and types of data that must be managed:

- Permissible demographic information
- Confidential data that is obtained through non-medical sources
- Opt-out records
- Authorizations provided by patients for additional PHI

All staff must know where these different types of data reside and who is authorized to access them.

Research and Reporting

The prospect researcher’s role as an information gatekeeper cannot be underestimated. The researcher sits at the center of several data streams:

- PHI
- Gift data
- Contact reports
- Public wealth and other information

Continued on following page

The experience and judgment of the researcher is the determinant of what information gets past the gate into the hands of development officers who will ultimately use that information to help them establish a meaningful and fruitful relationship with a donor. The ethical considerations are not unique to healthcare, but they are never more crucial than in the healthcare setting.

Given their special sensitivity to ethical and legal requirements for handling confidential information, prospect researchers are often the chief advocates for protection of donor privacy. Some researchers have observed that gift officers sometimes seem unaware or lack vigilance in respecting the laws and privacy of patients. This is not to unfairly single out major gift officers as being somehow unethical, but to recognize that, as humans, we can only keep so many issues top of mind. It often falls to prospect researchers to keep patient privacy top of mind and to remind, educate, and cajole the rest of the development staff when necessary regarding these important matters.

Back to Basics

Since targeted mass marketing is considerably more difficult for healthcare than it is for other types of nonprofits, fundraisers are finding that prospect research tools are more valuable to them than ever. There are two fruitful techniques that help to filter a large patient population using only the permitted demographic information. One approach uses models that identify the statistical profile of an organization's typical donor. The other is an automated matching process that screens patient names and addresses against public databases that might indicate wealth. By applying these filters, a fundraiser may make discrete and personal contact to explore the individual's interest in supporting the medical institution where he or she was served. This is another area where strong people skills, experience, discretion, and good institutional policy should govern when, where, and how such a contact should be made.

One of the unintended aspects of the legal restrictions on the use of patient information is that fundraising must emphasize relationships over marketing in the healthcare setting. This is, of course, at the very heart of the fundraising profession. People give to people, not institutions. It is the fundraiser's privilege and duty to seek out generous and capable people who want to help their fellow human beings. It is almost a form of midwifery. It is a personal act that happens one donor at a time.

About Blackbaud

Blackbaud is the leading global provider of software and services designed specifically for nonprofit organizations, enabling them to improve operational efficiency, build strong relationships, and raise more money to support their missions. Approximately 24,000 organizations — including The American Red Cross, Cancer Research UK, Earthjustice, International Fund for Animal Welfare, Lincoln Center, The Salvation Army, The Taft School, Tulsa Community Foundation, Ursinus College, the WGBH Educational Foundation, and Yale University — use one or more Blackbaud products and services for fundraising, constituent relationship management, financial management, website management, direct marketing, education administration, ticketing, business intelligence, prospect research, consulting, and analytics. Since 1981, Blackbaud's sole focus and expertise has been partnering with nonprofits and providing them the solutions they need to make a difference in their local communities and worldwide. Headquartered in the United States, Blackbaud also has operations in Australia, Canada, Hong Kong, the Netherlands, and the United Kingdom. For more information, visit www.blackbaud.com.

© August 2011. Blackbaud, Inc.

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

The information contained in this document represents the current view of Blackbaud, Inc., on the items discussed as of the date of this publication.

All Blackbaud product names appearing herein are trademarks or registered trademarks of Blackbaud, Inc. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.