ASA

Annie Searle & Associates LLC

Research Note

Privacy Policies and Public Awareness in the Healthcare Industry

By: Katharine Gallagher

Keywords: Privacy, Healthcare

Abstract: Technology has become a popular and convenient mode for delivering healthcare services. Self-service tools allow people to assess and proactively act upon certain aspects of their personal health and providers have learned that it is good business to reach out to patients when and where it is convenient for patients. However, some providers of these self-service tools do not always make it clear to people how their personal information is being stored, used, or if it will be passed on to a third party. There is no federal mandate that requires a business to have a privacy policy, but studies show that consumers are increasingly anxious about protecting their personal data.

Technology has become a popular and convenient mode for delivering healthcare services. Self-service tools allow people to assess and proactively act upon certain aspects of their personal health. Providers have learned that it is good business to reach out to patients when and where it is convenient for patients.[1] Today that could be through a smart phone application or at a grocery store, not just the doctor's office. The feedback from consumers with regard to these technologies has been positive and there are many businesses that are responding to this demand.

SoloHealth was founded in 2007 with the goal of providing free and convenient health information to the masses. Its principle product is a self-service kiosk that checks blood pressure, tests vision, measures body mass index, and delivers health risk assessments. The machine's user interface shows a person in a white coat with a stethoscope indicating the presence of a doctor, but the machine is not actually connected to a live doctor. The user is asked questions about personal and family medical history, diet, and mental health. The average user spends about 4.5

minutes at the kiosk and collectively these stations serve approximately 130,000 people each day for an average of 10 million customers each quarter.[2] The company has over 3,500 stations in popular stores such as Wal-Mart, Safeway, and Sam's Club.[3] All of the stations are strategically located to be within driving distance of 79 percent of the U.S. population.[4] In addition to providing the user with vital health information, the system also collects personal information such as names, email addresses, weight, age and ethnicity.[5]

When SoloHealth first started, it raised revenue by selling ad space for pharmacy items that were displayed in close proximity to the kiosks. However, as the business grew and the number of people using this product increased, the company soon realized that its most valuable asset was the health and personal data it collected from its customers. This wealth of information is attractive to businesses within the health industry, particularly insurance companies.

In 2014, *National Public Radio* (NPR) in conjunction with *Kaiser Health News*, ran a story about SoloHealth claiming that it was not being forthright with consumers about the data it collects, stores, and sells. According to NPR, until recently SoloHealth's comprehensive privacy policy was not available at any of the stations; it was only obtainable on its website.[6] The company provided its website address at the kiosk, but since the stations do not have internet access, there is no way for anyone to actually read the policy prior to using the machine. SoloHealth claims that it did not provide access to its privacy policy because it would be burdensome for consumers to read the information on the kiosk's small computer screen. NPR says the company only sells "names, email addresses, and phone numbers to insurers who want to market health plans directly to consumers."[7] However, *Kaiser Health News* asserts in a separate article "all information, except the email addresses, is aggregated and shared with SoloHealth sponsors without personal identifiers."[8] The conflicting reports lead one to question how patience information is actually being handled and whether personal data is truly being separated from health data.

Some doctors' groups and privacy advocates wonder how the health data collected by these tools could be used, or rather misused, in the future. Many people consider their health information to be private. Something as sensitive as this should be protected and there should be control over who gets to see it and what aspects can be disclosed. When a person visits a doctor, it is common knowledge that he or she is protected by a patient physician confidentiality agreement. The Health Insurance Portability and Accountability Act (HIPAA) ensures that people are able to keep individual health information private. Under its notice of privacy practices, it is stated that a person's health information cannot be used for purposes not directly related to his or her care without permission. It also states that one may ask that health information not be shared with other individuals or companies.[9] SoloHealth is not considered a covered entity under HIPAA law, but its practices are questionable and should be reviewed by a regulatory agency.[10] Users of SoloHealth's product may be under the impression that information conveyed at the kiosk is just as secure as it is in a doctor's office due to the personal nature of the questions they answer, but that is not the case. This reinforces why it is vital for consumers to have the right to know who else may be privy to their data.

In mid-December of last year, SoloHealth finally made its comprehensive privacy policy available at its kiosks. This was an effort to be more transparent. Bart Foster, SoloHealth's CEO, said, "we work with retail partners, our attorneys and our corporate sponsors to make sure that we're totally buttoned up."[11] That begs the questions: Is the privacy policy designed to protect the consumer or the business? Is it the responsibility of the business to be more transparent? Or is the onus on the consumer to understand that any or all of the information provided may be passed along to a third party?

A privacy policy explains what data is collected by a business, how it is stored, used, and distributed. Many companies with an online presence have them, but there is no federal mandate that requires a business to have one. In fact, privacy policies can be considered part of a company's marketing strategy, a public relations move to make a consumer feel that his or her

search and personal data are protected. They give the impression of security; however, often times, when the policy is actually read there is very little protection being promised.[12] The Federal Trade Commission only steps in to regulate if a company does not conform to the mandates that are outlined in its policy, otherwise the world of privacy policies is self-regulating.

From a behavioral economics perspective, many studies indicate that consumers are becoming increasingly anxious about protecting their personal data. However, despite this, many people are still not likely to read online privacy policies, or even understand them.[13] In addition, the presence of a privacy policy may be interpreted as protection even if the information disclosed in the policy indicates otherwise.[14] Given the outcome of these studies, businesses know that they still have the upper hand. Privacy policies provide a level of protection for companies; they can lay out exactly how consumer data is collected and used, knowing that most people won't even bother to read about it. This leaves companies with an ethical duty to explain in a clear and concise manner how a consumer's data is collected, stored, and distributed. This information should also be easily accessible, not buried at the bottom of a website.

In a situation where a service is provided free, such as with SoloHealth, the notion of caveat emptor certainly applies. Health information is paid for through the exchange of personal information. When people voluntarily provide information, there is no guarantee of privacy protection. Although a customer may find it acceptable to trade this information with a business, he or she should absolutely be notified about the fact that this information may not be entirely private before the exchange occurs. In a world where so much personal data is stored in databases or in the cloud, consumers need to be educated on the ramifications of big data in a manner that is easy to understand. There is, without a doubt, great benefit from collecting and analyzing personal data; it simplifies a person's life and provides fast and individualized assessments. In contrast, the massive amounts of data that can be easily obtained about an individual are unsettling. A balance must be found between the risk and the reward. In this age many would not give up the everyday conveniences provided by technology, but in the campaign

to promote privacy awareness, the best hope is to inform people how data is being used and present people with the choice of whether to participate.[15] This is best facilitated by the entity that is asking for the information.

The concept of privacy is a gray area. Disagreements over its scope and meaning make it difficult to establish a definition that everyone can agree upon. The notion of privacy will vary depending on how and where a person grew up and is shaped by personal experience. There is, however, one aspect of this subject that should be black and white and that is upfront and full disclosure in a "simplified and human-friendly manner" of how a person's data is shared with other parties.[16] Through this practice, people can be educated on how businesses use data to understand their customers. Consumers can then decide for themselves what their level of comfort is on the privacy spectrum and be empowered to proceed in the manner they deem best.

---

[1] Dowling, Jim. "A Convenient Truth: Self-Service Works in Healthcare." *Healthcare IT News*. 31 Oct. 2013. Accessed Feb. 2014 <www.healthcareitnews.com>.

[2] "SoloHealth Station Surpasses the 40-Million Mark for Consumer Engagements; Now in More Than 3,500 Retail Locations Nationwide." *PR Web*. 20 Dec. 2013. Accessed Feb. 2014 <www.prweb.com>.

[3] Ibid.

[4] Dearment, Alaric. "About 130,000 People Use SoloHealth Stations Per Day, Company Says." *Drug Store News*. 20 Dec. 2013. Accessed Feb. 2014 <www.drugstorenews.com>.

[5] Dembosky, April. "After Checking Blood Pressure, Kiosks Give Sales Leads To Insurers." *National Public Radio*. 15 Jan. 2013. Accessed Feb. 2014 <www.npr.org>.

[6] Ibid.

[7] Ibid.

[8] Appleby, Julie. "Health Care Without the Doctors Coming to a Wal-Mart Near You." *PBS Newshour*. 20 Dec. 2013. Accessed Feb. 2014 <www.pbs.org>.

[9] "Your Health Information Privacy Rights." U.S. Department of Health and Human Services. n.d. Accessed Feb. 2014 <www.hhs.gov>.

[10] Appleby, Julie.

[11] Dembosky, April.

[12] Nehf, James P. "Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy." *University of Illinois Journal of Law, Technology & Policy*. Jan. 2005. Accessed Feb. 2014 <www.illinoisjltp.com/journal>.

[13] Haynes, Allyson W. "Online Privacy Policies: Contracting Away Control Over Personal Information?" *Penn State Law Review*. 1 Jan. 2007. Accessed Feb. 2014 <www.pennstatelaw.psu.edu >.

[14] Acquisti, Alessandro., et al. *Digital Privacy: Theory, Technologies, and Practices*. Auerbach Publications. 2007.

[15] Sengupta, Somini. "Letting Down Our Guard with Web Privacy." *New York Times*. 30 March 2013. Accessed Feb. 2014. <www.nytimes.com>.

[16] Steinberg, Joseph. "This Flashlight Android App Has Been Secretly And Illegally Sharing Your Personal Data With Advertisers." *Forbes*. 16 Dec. 2013. Accessed Feb. 2014 <www.forbes.com>.