Privacy Safeguards in PHR Adoption

By Wendy Angst

Several incidents of recent years explain why healthcare consumers remain concerned about the privacy, security and confidentiality of their personal health information. In 2006, a database containing sensitive information about veterans and their families was stolen after a U.S. Department of Veterans Affairs employee violated policy and took the data home. In 2007, a security lapse exposed the personal information of more than 9,000 Concord (New Hampshire) Hospital patients, leaving their names, addresses, dates of birth and Social Security numbers unprotected on the Internet.

Also in 2007, Palisades Medical Center in California suspended 27 of its employees for accessing the medical records of actor George Clooney without obtaining clearance.

Such highly publicized stories illustrate why many consumers remain skeptical of adopting and using electronic databases for maintaining personal health information, or personal health record (PHR) products, especially when these databases are maintained by third parties. And yet, there are many things healthcare organizations offering PHRs can do to alleviate consumers’ distrust and skepticism over privacy issues and thereby increase the adoption and use of PHRs.

Privacy

More than ever, organizations must demonstrate their strict adherence to privacy principles, policies, practices and training. Patients increasingly perceive privacy breaches as a form of already pervasive identity theft. The problem is so serious that Patient Privacy Rights, a non-profit organization located in Austin, Texas, dedicated to ensuring the security of patient health records, will soon evaluate electronic health record products (including PHRs), awarding seals of approval to those that meet standards for protecting the privacy of consumers’ information.

Add to this the prospect of financial risk. For example, the New York Supreme Court Appellate Division, in 2007, ruled that a patient could receive $300,000 in punitive damages, plus $65,000 in compensatory emotional distress, for a negligent breach of confidential medical information.

Many compare the needed security and privacy policies to that of the financial industry. Consumers are becoming increasingly familiar with the risks of identity theft and fraud thanks to clever advertising campaigns and the unfortunate experiences of others. As with the financial industry, consumers can be made “whole” (not counting the enormous inconveniences) with compensation. However, when it comes to an individual’s personal health information being improperly disclosed, it is virtually impossible to right the wrong. Taking every recommended precaution on data privacy and security is necessary, but it is never enough. Healthcare consumers expect more, and healthcare organizations that want to succeed in the marketplace must be prepared to deliver.
educating consumers about those safeguards are key to alleviating consumer concerns and boosting adoption rates.

A Core Concern

Consumers' top concern about PHRs is the potential misuse of health record data, according to a 2006 study from the Markle Foundation. Eighty percent of those surveyed reported concerns with identity theft and fraud, while 77 percent were worried that data could get into the hands of marketers, or employers (56 percent) and insurers (53 percent). Strong predictors of PHR use include education and knowledge of how PHRs work, convenience, compliance and connectedness, according to research from the Center for Health Information and Decision Systems at the University of Maryland.

The research claims that consumers who are likely to opt out of PHRs due to an attack of privacy anxiety may also be willing to relinquish some privacy in exchange for the promise of better care. The key rests in creating strong messages that outline how and why care will improve through PHR adoption and use.

What Must Be Done

Organizations should carefully review PHR end-user agreements for adequacy of consumer controls and secondary data uses, and support organizations that advocate innovation and change in privacy policy and practice. The best PHRs offer consumers flexibility and a high level of control over the information they choose to share with care providers and family members. Rather than resorting to a PHR that grants blanket access to personal information, consumers should be able to limit access to information on a specific condition or to information within specific categories such as tests, treatments or medications. The “Coalition for Patient Privacy” laid down similar principles in 2007, arguing that consumers have “the right to segment sensitive information” and maintain “control over who can access their electronic health records.”

Of equal concern is the use of secondary data, now being addressed through the American Medical Informatics Association’s (AMIA) initiative to develop a national framework for secondary use of health data. Such a framework will include components such as transparent policies and practices, a focus on data control versus ownership, consensus on privacy policy, security and public awareness campaigns, as reported in ‘Toward a National Framework for the Secondary Use of Health Data,” published by AMIA in 2006.

There are many things healthcare organizations offering PHRs can do to alleviate consumers’ distrust and skepticism over privacy issues and thereby increase the adoption and use of PHRs.

Organizations must develop a strong PHR education and promotion program and include health improvement messages that help consumers minimize privacy worries and assume reasonable privacy risks. Among the potential core messages to consider are: improving patient health and the health of loved ones through reminders and alerts on preventive and follow-up care and compliance; saving time and improving health outcomes by avoiding the burden of trying to recall essential medical information during appointments and emergencies; enhancing communication with care team members, providers and family members; and, managing a patient's condition and health by accessing personally tailored health information and resources.

Organizations should also follow the lead of entities such as the American Health Information Management Association, which recently revamped an educational program covering issues such as
the prevention and treatment of medical identity theft, notices of privacy practices, informed consent, authorization for release of information, and access to children’s health records. Likewise, the new privacy toolkit of the Patient Privacy Rights organization addresses issues such as physician-patient conversations on physicians, consumer privacy rights, how to file a privacy complaint and participating in national programs to safeguard privacy.

In addition to covering issues such as personal rights and responsibilities, privacy policies, permissible data uses and opt-out provisions, organizations should incorporate recommendations from the World Privacy Forum, which counsels consumers to combat medical identity theft through regular review of medical records and insurance payments.

Organizations must also insist upon sound, up-to-date privacy policies. According to a 2007 report completed by Altarum Institute for the Office of the National Coordinator for Health Information Technology, the privacy policies of the majority of PHR vendors are incomplete. Vendors often lack privacy policy requirements and standards, especially in areas such as secondary use of data, data disposal and personal information definitions.

Federal Regulations and State Law

While some PHR privacy policies address issues such as IP addresses and cookies, use of information provided at registration, links to other sites, HIPAA choice and opt-out, corrections as well as updating and removal of data and notification of changes, organizations must go farther. Privacy policies must follow the guidelines of the American Health Information Community and deliver clear, understandable information on privacy policy effectiveness dates, policy changes, secondary uses of data, business and financial relationships, special protections for minors, federal rules and regulations and common PHR terminology.

Organizations also should prepare a crisis management plan to cope with privacy breaches. For example, in January 2008, Blue Cross Blue Shield of New Jersey quickly notified its members when an employee laptop computer containing personal information for about 300,000 individuals was stolen. It explained how a security procedure had already destroyed all data on the stolen computer and then offered affected members complimentary credit monitoring services for one year.

Not all organizations will respond the same way, which is why they must first study state privacy breach laws, as well as emerging trends in privacy breach reporting. For example, California privacy breach laws that went into effect Jan. 1, 2008, redefined and broadened the definition of personal health information. Nonetheless, every organization will benefit from a crisis communications plan emphasizing core values such as timeliness, candor and clarity, support for coping with problems associated with the breach and careful documentation of the breach incident.

As the number and types of PHRs proliferate, consumers may become even more confused about the strengths and weaknesses of these electronic records. Champions and sponsors of the technology can help to manage consumer chaos through sound privacy policies and practices, diligent privacy reviews of the products, PHR privacy education and communication planning for possible privacy breaches. The overall value that can be gained by using an electronic health record far outweighs the risks. The onus is on the suppliers of PHR applications to ensure that consumers can engage with this technology with a sound peace-of-mind.

Wendy Angst is general manager of CapMed, a division of Bio-Imaging Technologies and provider of interactive personal health management solutions
based in Newtown, Pa. Contact her at Wangst@capmed.com.