By Barry P. Chaiken, MD, FHIMSS

We Need Privacy Now

Pri•va•cy (n)
The condition of being concealed or hidden.

Although a simple definition, it captures our greatest concern about the digitization of our medical information. Who will access my medical record? Will the information be used against me? Will it be released on the Internet?

In the Bill of Rights, the Fourth Amendment to the U.S. Constitution states:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Although written to restrict the reach of the government into the lives of the people, the amendment represents our basic expectation of privacy in our lives across all aspects of society. Over the past 220 years, this expanded concept of privacy has become a fundamental right—woven into the fabric of our culture—that does not exist in any other country in the world.

Privacy of medical records is not a new problem brought on by information technology. Even with paper records, unauthorized access to patient information frequently occurred. During my clinical training, patient records were readily available at the nurses' station on each ward. Anyone working in the hospital could easily walk up to the chart stand, pull a record and read freely whatever they wanted. On occasion, an attending would walk off with a chart, requiring a mad search for it by the ward clerk. Over time, procedures were put in place to offer better control of access and therefore privacy, of the patient record. Even with these changes, the record was never kept fully private.

Privacy of medical records is not a new problem brought on by information technology.

Restricted Access

Electronic patient data may present a more challenging environment of maintaining privacy of patient records, but the fundamental principles remain the same. Ensuring privacy of medical records requires that access to a patient's record be restricted to those individuals that need access to provide appropriate care to the patient. If access to the record is not for the purpose of providing benefit to the patient, then access should be restricted.

The digitization of all data in our society makes privacy of medical records extremely difficult. With digitization comes the ability to easily copy, transfer, and access large amounts of information cheaply.

In the realm of healthcare, patient information exists in many forms beyond that of the patient record. Pharmacy, laboratory, and radiology databases feed information into the patient record while standing alone as sources of patient data. Payors and medical benefits managers, among others, store patient medical information, which they use in the operation of their businesses. Research databases, built from patient data, provide academics with valuable raw material, which helps fuel their scientific pursuits. In some cases, this data is de-identified immediately (e.g., population research database) while in other situations it is de-identified after its intended use to complete a particular task (e.g., insurance claim).

De-identification Myth

Any feeling of comfort associated with the de-identification of data is alarmingly a false feeling. Re-identifying patient information is a relatively straightforward activity. For example, reverse lookup databases can easily link an address, social security number, or even an employer/job title to an individual. They may not work perfectly all the time, but they re-identify well enough that corporations frequently use them

In the realm of healthcare, patient information exists in many forms beyond that of the patient record.

to identify potential customers or target market products.

More than two years ago, I warned that for-profit entities might use private patient data to market products to consumers.

> *Patient data may be used to target relevant product ads to individuals based upon the data contained in the medical record (Chaiken, 2007).*

Today, patient information is actively being used to target market products and services to patients. Large pharmacy chains such as CVS Caremark and Walgreens regularly utilize pharmacy information to identify patients to whom they send out email messages, coupons, and flyers. Although the data they utilize is de-identified, they employ these reverse lookup utilities to reconstruct the information with patient identifiers.

Even with the privacy restrictions enacted in the American Reinvestment and Record Act 2009 (ARRA), the improper use of patient data—defined as the use of restricted patient data, without permission, for purposes other than that related to the direct care of the patient—will continue to grow at a quickening rate.

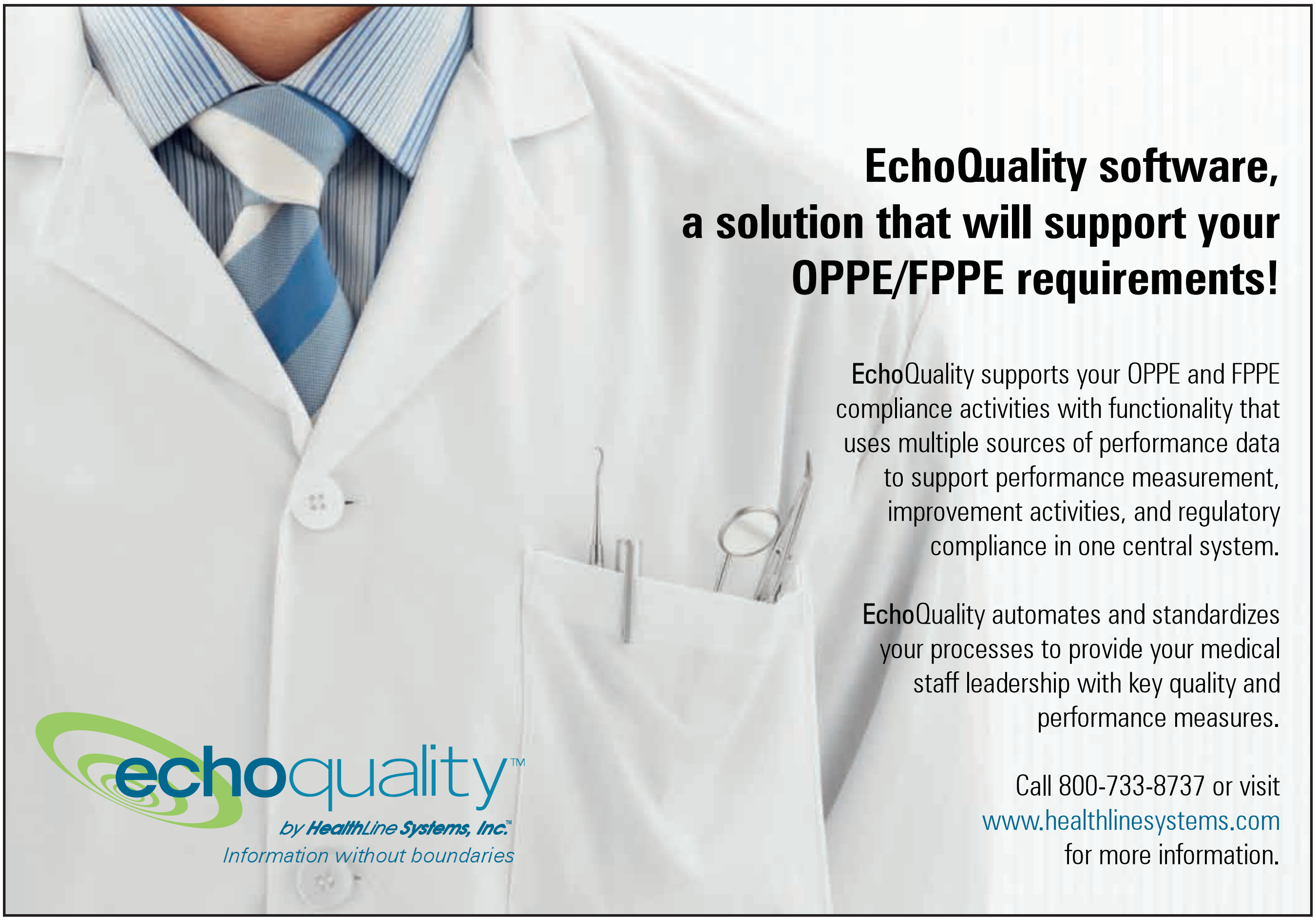
At a meeting with several health information technology leaders at the HIMSS 2008 Annual Conference, Google's CEO, Eric Schmidt, was cautioned about the use of patient data contained within Google Health. Although WebMD and Microsoft currently acknowledge the privacy rules outlined in ARRA apply to them, Google disagrees. *The New York Times* quoted a representative of Google in an article published this summer, who said:

> *Google is bound by the privacy policy that people agree to when they sign up (Freudenhein, 2009).*

WOW. To this day I still have not met anyone who reads those legal notices we all are asked to accept before using software or accessing certain websites. To rely on the acceptance of the privacy policy upon sign up as a defense for using patient information in any commercial way deemed appropriate seems weak and suggests exploitation.

Benefits to Data Exchange

Patient data must be shared to achieve both personal and societal goals. Facilitating the exchange of patient information among providers works to improve quality, ensure safety, and reduce costs. Although it is true that we have not achieved to date anywhere near the benefits we envision



from this exchange, brilliant and dedicated informaticists, clinicians, and process engineers are working on the right problems and achieving incremental improvements. As discoveries are made, best practices spread and benefits accrue.

Society obtains great benefit through the generation of research databases that are mined to learn more about disease processes and relevant treatments. In addition, these large databases provide disease surveillance data for public health entities looking for outbreaks or acts of bioterrorism. They also offer policy makers data necessary for healthcare planning.

With all of the benefits offered by electronic patient data comes the risk of inappropriate and exploitive use. The privacy rules developed from the ARRA legislation must protect patients from unwanted marketing of products and services generated from their own medical data. In addition, severe financial and criminal penalties must be established for the violation of the privacy of patient data to properly incent payors, providers, benefits managers, and other commercial entities to protect and properly use patient data. Only with strictly enforced privacy rules can healthcare information technology provide the quality, safety, and costs benefits expected from its deployment.

Patient data must be shared for us to achieve both personal and societal goals.

***Barry Chaiken** is the chief medical officer of DocsNetwork, Ltd. and a member of the Editorial Advisory Board for* Patient Safety & Quality Healthcare. *With more than 20 years of experience in medical research, epidemiology, clinical information technology, and patient safety, Chaiken is board certified in general preventive medicine and public health and is a Fellow, Board Member, and Chair of HIMSS. As founder of DocsNetwork, Ltd., he has worked on quality improvement studies, health IT clinical transformation projects, and clinical investigations for the National Institutes of Health, U.K. National Health Service, and Boston University Medical School. Chaiken also serves as an adjunct assistant professor in the Department of Public Health and Family Medicine at Tufts University School of Medicine. He may be contacted at bchaiken@docsnetwork.com.*

References

Chaiken, B. P. (2007). Patient information: Who's your daddy? *Patient Safety & Quality Healthcare, 4*(5), 6–7.

Cornell University Law School. Legal Information Institute. United States Constitution. *Bill of Rights.* Available at http://www.law.cornell.edu/constitution/constitution.billofrights.html#amendmentiv

Freudenheim, M. (2009, August 8). And you thought a prescription was private. *The New York Times.* Available at http://www.nytimes.com/2009/08/09/business/09privacy.html?scp=1&sq=&st=nyt