

## Patient Information: Who's Your Daddy?

Try “Googling” yourself. What did you find? Anything that you really wish was not for everyone to see on the Internet? Perhaps that horrible high school mug shot from your yearbook popped up. With luck, you did not have your social security number appear, too.

Throughout our industry, leaders promote the virtues of electronic medical records, and the easy exchange of digital data to assist in providing patient care. According to many of these experts, the elimination of paper records brings improved quality of care, enhanced patient safety, and saves billions of healthcare dollars. Considering the \$2 trillion size of the healthcare industry, many companies see huge business opportunities in collecting and managing electronic patient data.

As healthcare organizations move forward with deploying electronic medical records, they continually struggle with the appropriate governance structure necessary to manage the access and handling of patient information. In other words, no widely accepted, clear standards exist to guide organizations on who can access patient information, how they secure permission to access it, and what they can do with it. Without very specific rules and strict oversight, it is likely that some patient-specific medical information may actually appear after

**Multiple options exist for management of electronic patient information, with each having positive and negative aspects.**

use of Internet search engines such as Dogpile, Yahoo! Search, and Google, among others.

### **Patients Own the Information**

Although patients own their medical information, they do not own the paper, servers and CDs on which it is stored. Patients have rights to obtain their medical information in a timely manner, which in some organizations that employ paper records can take 90 days to get copied and delivered to the patient. With digital patient information, the time and cost associated with printing out a medical record is reduced, but the issues of permission to access and timely retrieval still remain. Patients need to choose their approach to managing their electronic medical record wisely as the available options are numerous, and each has far-ranging implications for the privacy and security of their medical record.

### **Multiple Data Ownership Options**

Multiple options exist for management of electronic patient information, with each having positive and negative aspects.

#### **Patient**

Managing their own data affords patients the highest level of control over that information but presents significant obstacles to those needing to access it (e.g., physicians, nurses, emergency medical personnel). Various methods of patient ownership exist including smartcards, flash drives, and implantable RFID chips. These options require the acceptance of data and technology standards as well as the widespread distribution of devices compatible with the format of the electronic information.

#### **Payor**

Payors currently possess the most extensive database of electronic patient information obtained through their claims processing activities. Historically, patients have been less trusting of payors to keep their patient data confidential. In addition, many patients fear that their data will be used to their disadvantage in health coverage, disability, and life insurance decisions.

#### **Provider**

Providers may have the largest amount of clinical patient information, but it is fragmented across providers, stored in incompatible formats, and often exists in non-electronic form (e.g., paper charts in physician offices). Through the development of health information exchange standards (e.g., Health Information Technology Standards Panel [HITSP]; the Continuity of Care Record), strides are being made to facilitate interoperability and health information exchange. Although providers are considered trusted custodians of patient information, challenges of availability and lack of completeness continue to prevent providers from supplying comprehensive patient medical records.

#### **Trusted Authority (Non-Profit)**

Over the past several years Regional Health Information Organizations (RHIOs) have formed to provide a trusted authority to manage the exchange of electronic medical information among providers. Whether a federated model, where information resides on disparate provider computers, or a centralized model, where patient data is aggregated into a single record, challenges of governance, interoperability, and funding continue to present themselves.

There is no guarantee that the data will solely be used for purposes that benefit consumers.

#### **For-Profit Entity**

Both Microsoft and Google are forging ahead with plans for online electronic medical records that are populated and managed by each individual. Other organizations such as WebMD and Revolution Health already offer their own versions. Microsoft and Google intend to provide them free or at a nominal fee, while each plans to use the data collected for a variety of still undisclosed business purposes. Patient data may be used to target relevant product ads to individuals based upon the data contained in the medical record (For example, overweight people are targeted with weight-loss medications or diet plans.)

#### **Government**

Both the federal and state governments in the United States refrained from building a data repository for electronic medical information. Even in the United Kingdom, where single payor universal healthcare coverage has existed for decades, there is growing concern about the building of a centralized longitudinal care record as part of the recent investment in healthcare information technology in England.

#### **Patients are Responsible**

The ultimate responsibility for managing our electronic medical information falls to each of us. Acting passively and allowing others to decide for us how our information is accessed and used guarantees that those decisions will not be in our best interest. Only through a strict governance structure that balances our right to privacy while ensuring reasonable access to facilitate our care and promote community wellness (e.g., access for medical research purposes that also protects our privacy) can we be assured that

our information is only used for our own benefit.

Most disturbing of the several options noted above is the control of medical records by for-profit entities. This control provides these organizations with significant business opportunities that may offer little benefit to those whose data is being exploited. In addition, there is no guarantee that the data will solely be used for purposes that benefit consumers. What would prevent the organization from targeting ads for unproven medical remedies to specific consumers? And who would determine whether the remedies are unproven?

So where does all this leave us? All potential options for managing our electronic medical data present significant risks, yet the potential benefits are significant. Without unwavering confidence in the entity that will manage our patient information, most consumers will be reluctant to provide complete and accurate data. Only through the establishment of a respected authority with rigorous and transparent oversight can we produce an environment where consumers will openly share their precious medical information.

Some characteristics of such an organization include:

- Local control through a board of trustees chosen from the community.
- Security and privacy rules established through legislation with severe penalties for any breaches.
- Status as a non-profit, privately run entity.
- Independent security and privacy advisory committee providing constant oversight.

No matter whether the entity that manages our electronic medical records is provider or payor, for-profit or non-profit, Web-based or stored locally, a powerful oversight entity must exist to ensure adherence to an ironclad governance structure that

protects our medical privacy while ensuring that our information is available to make and keep us well. **IPSQH**

**Barry Chaiken** has more than 20 years of experience in medical research, epidemiology, clinical information technology, and patient safety. As founder of his own company, he has worked on quality improvement studies and clinical investigations for the National Institutes of Health, Framingham Heart Study, and Boston University Medical School. Chaiken is board certified in general preventive medicine and public health and is a Fellow and Board Member of HIMSS. He is the associate chief medical officer of BearingPoint, Inc., adjunct assistant professor in the Department of Public Health and Family Medicine at Tufts University School of Medicine, and serves on the Editorial Advisory Board for Patient Safety and Quality Healthcare. He may be contacted at [bchaiken@docsnetwork.com](mailto:bchaiken@docsnetwork.com).

#### **FURTHER READING**

- Chaiken, B. P. (2007, March/April). Are interoperability and privacy compatible? *Patient Safety and Quality Healthcare*, 4(2), 8-9.
- \_\_\_\_\_. (2006, July/August). Interoperability: Finding a home for your data. *Patient Safety and Quality Healthcare*, 3(4), 10-11.
- \_\_\_\_\_. (2005, September/October). Interoperability: More knowledge or just more data. *Patient Safety and Quality Healthcare*, 2(5), 6.
- \_\_\_\_\_. (2005, July/August). Consumer-directed healthcare. Increasing demand for quality data. *Patient Safety and Quality Healthcare*, 2(4), 6-7.
- \_\_\_\_\_. (2004, October/December). Continuity of care record: Foundation for quality. *Patient Safety and Quality Healthcare*, 1(2), 12-13.
- Lohr, S. (2007, August 14). Dr. Google and Dr. Microsoft. *The New York Times*, C1, C8, NYC Final edition.