
 EDITORIALS

Can You Keep a Secret?

Measuring the Performance of Those Entrusted With Personal Health Information

The headlines in *The Washington Post* screamed about hackers breaking into hospital computer systems in Seattle¹ not too long after headlines told of marketing firms calling customers on behalf of drugstore chains to remind them to refill their prescriptions. Who could blame the public for wondering who has access to confidential personal health information and what they might do with it?

The fear that putting sensitive personal information into a computer places it at risk is contraposed by the belief that programmers can create computer firewalls, anonymize and de-identify data, and make it safe from prying eyes.

This would give the impression that concern about the privacy and confidentiality of personal health information is a creature of the era of electronic information. This image — of breaches in confidentiality being just another moving violation on the information superhighway — couldn't be more misguided. Any of us who recited the Hippocratic Oath at medical school graduation repeated an ancient Greek pledge to "hold in confidence all that my patient confides in me." But few of us who have ridden an elevator in a busy hospital could have been surprised by Peter Ubel's finding that in one of every seven elevator rides a hospital worker comments about a patient in a way that is inappropriate, often revealing confidential and sensitive information.²

It should be no wonder, then, that the public expresses little faith in our ability to keep a secret. According to a survey conducted by the Gallup Poll for the Institute for Health Freedom in September 2000, over 70% of respondents were opposed to giving doctors free access to their medical records. Over 90% were concerned about government agencies and almost 70% about researchers.³

President Clinton's Advisory Commission on Consumer Protection and Quality in the Healthcare Industry recognized how strongly the public feels about its privacy. In November 1997, it listed "Confidentiality of Health Information" as one of eight areas of rights and responsibilities: "Consumers have the right to communicate with health care providers in confidence and to have the confidentiality of their individually identifiable health care information protected."⁴

Who will serve as the protector of personal health information? As Wynia et al. describe in this issue,⁵ Federal efforts to safeguard sensitive information go as far back as the 1973 report to the Department of Health,

Education and Welfare that led to the 1974 Privacy Act. More recently, Congress made confidentiality a key element of the 1996 Health Insurance Portability and Accountability Act (HIPAA) and mandated that, if legislation protecting privacy in electronic data interchanges were not passed by August 21, 1999, the Secretary of Health and Human Services must issue regulations to protect it.

In a speech at the National Press Club in July 1997, Donna Shalala laid out a conceptual framework for Federal safeguards of health care information, which is based on five principles:

1. **Boundaries:** With very few exceptions, personal health information should be disclosed solely for health care purposes.
2. **Security:** Patients should feel that their personal medical information is secure.
3. **Consumer Control:** Patients should have access to their medical records and be able to correct information that is incorrect.
4. **Accountability:** Persons who misuse personal medical information should be severely punished.
5. **Public Responsibility:** A balance needs to be struck between the right to privacy and the support of national priorities, especially four — research, quality of care, public health, and the commitment to prevent fraud and abuse.

Because the Congress did not pass privacy protections by its self-imposed deadline, the Department of Health and Human Services (HHS) published a proposed regulation on November 3, 1999.⁶ The proposed regulation specified what information would be covered, under what circumstances personal health information could be disclosed, and how much information could be disclosed. About 52,000 comments were reviewed, and a final regulation was prepared, which was released on December 10, 2000.

Regardless of the lengthy details of the Federal privacy regulations, there will be a need for private sector leadership in setting standards, both for complying with the regulations and for ensuring the confidentiality of records in ways the regulation does not address. A few healthcare organizations have developed standards for research and health care practice, and model language has been

proposed for state laws on privacy.⁸ An Institute of Medicine committee chaired by Bernard Lo, funded by the Agency for Healthcare Research and Quality and the HHS Assistant Secretary for Planning and Evaluation, has proposed an agenda to help Institutional Review Boards (IRBs) fulfill their responsibility for overseeing the use of personal health information in research.⁹

This is why the article by Wynia et al. is so important. The E Force (Ethical Fundamental Obligations Report Card Evaluations) Program represents an admirable commitment by many stakeholders, especially the American Medical Association (AMA), to provide leadership in the ethical conduct of health care. As it did when it established and provided early support to the National Patient Safety Foundation, the AMA seems to be recalling the hopes of its founders like Nathan Davis that it would offer professional standards and leadership to improve the quality and ethical standards of American medicine. The E Force standards offer a benchmark against which clinicians and health care organizations can measure their performance, identify where they may fall short in ensuring confidentiality of personal health information, and plan improvement.

I must declare my lack of impartiality on this count. As a member of the E Force Oversight Body, I was impressed by the cautious and thoughtful way in which this consensus document was assembled. The consensus included a variety of stakeholders in health care — business and labor, patient advocacy groups and oversight organizations, public hospitals and private health plans, integrated delivery systems and health professionals.

The E Force consensus document on confidentiality is important for another reason. The HIPAA standards and state privacy laws establish a regulatory and legal framework for privacy. The E Force document and professional society guidelines offer an ethical framework for privacy. However, the E Force standards go a step beyond regulation and professional ethics to recognize the power of the market in health care. By establishing standards for privacy, the E Force document offers the public a measuring stick to gauge how well health care providers and health plans are guarding personal health information. If the E Force standards are adopted as performance measures, then not only will providers and plans know how they will be measured, but also their clients will know how well they are measuring up.

This will be one of E Force's most important contributions — to take ethical practice beyond professional responsibility and legal compliance into the world of health care markets and to empower patients and purchasers with information to guide their choices. A market cannot work effectively without meaningful consumer choice, and choice is meaningless without good information. If the health care market works as it should, then the public's expectations will find voice in choice, and providers will find that there is a business case, as well as

a professional and legal case, to be made for ethical practices.

The E Force standards also make substantive contributions to the way that health care information can remain confidential. They include 34 measurable expectations in eight areas: transparency; consent for use and disclosure; limitations on information that can be collected and by whom; individuals' access to their own records; security of storage and transfer; data quality; limitations on how the data can be used; and accountability.

The E Force standards introduce several important concepts. First, a health information trustee who is responsible for implementing security mechanisms and processes offers a practical way to operationalize a set of ethical principles. Second, every organization that handles personally identifiable health information, whether a health plan, hospital, physician or pharmacy, should consider itself a health information trustee and adhere to these shared ethical norms. Third, a publicly accountable process to authorize waivers of individual consent makes personal health data available in a way that is responsive to the public good in using the information while honoring the individual's interest in privacy. Fourth, using Institutional Review Boards (IRBs) for research waivers and a data disclosure board or privacy board for instances in which an IRB would be inappropriate offers a structure for oversight without overburdening IRBs, and makes clear that every organization should have an identifiable individual or team responsible for adherence to confidentiality standards. Fifth, a set of standard and consistent practices and policies that these boards may follow avoids each board having to invent the standards itself. Sixth, the E Force document recognizes the importance of training for those who will collect, store, and use identifiable health information. Seventh, it proposes that organizations be clear and transparent about the procedures it uses to de-identify data for uses such as quality assurance and research. Eighth, and finally, it recommends the design and use of Data Needs Assessment and Privacy Impact Assessment documents, which would, like the rest of the recommendations, offer much needed predictability and consistency to the process of waiving individual consent.

The E Force Program's recommendations on the protection of identifiable health information, coupled with the final HIPAA regulation, allow the nation to keep personal health information confidential but not buried. They offer a chance to lock up our most sensitive health information, but not to throw away the key. They offer a challenge to researchers, public health officials, and others responsible for quality assurance and quality improvement, as well as to clinicians and their institutions, to use sensitive information prudently. Only then will the public conclude that its personal health information is safe, and that it need not fear that its information will be misused.— **JOHN M. EISENBERG, MD**, *Director, Agency for Healthcare Research and Quality, United States*

Department of Health and Human Services, and former Chairman, Department of Medicine, Georgetown University Medical Center, Washington, DC.

The views and opinions expressed in this editorial are those of the author and do not necessarily represent policies of the Agency for Healthcare Research and Quality nor the Department of Health and Human Services.

REFERENCES

1. "Hacker Accesses Patient Records," Washington Post December 9, 2000, page E1.
2. Ubel PA, Zell MM, Miller DJ, Fischer GS, Peters-Stefani D, Arnold RM. Elevator talk: observational study of inappropriate comments in a public space. *Am J Med.* 1995;99:190-4.
3. Institute for Health Freedom. Public Attitudes Toward Medical Privacy. Report submitted by the Gallup Organization. Princeton, NJ: September, 2000 (available at www.forhealthfreedom.org/Gallupsurvey/).
4. The President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry. *Quality First: Better Health Care For All Americans.* Final Report to the President of the United States. Washington, DC: United States Government Printing Office; 1998:A-57.
5. Wynia MK, Coughlin SS, Alpert S, et al. Shared expectations for the protection of identifiable health care information: report of a national consensus process. *J Gen Intern Med.* 2001;16:100-11.
6. Standards for Privacy of Individually Identifiable Health Information: Proposed Rule. Washington, DC: 64 Fed. Reg. 59918; 1999. (available at <http://aspe.hhs.gov/admsimp/>).
7. Department of Health and Human Services. Protecting the privacy of patients' health information. Summary of the final regulation. HHS Fact Sheet. Washington, DC: U.S. Department of Health and Human Services; 2000 (available at <http://aspe.hhs.gov/admsimp/pvcfact1.htm>).
8. Hodge JG Jr, Gostin LO, Jacobson PD. Legal issues concerning electronic health information: privacy, quality, and liability. *JAMA.* 1999;282:1466-71.
9. Committee on the Role of Institutional Review Boards in Health Services Research Data Privacy Protection. *Protecting Data Privacy in Health Services Research*, Division of Health Care Services, Institute of Medicine. Washington, DC: National Academy Press. In press (available at http://books.nap.edu/html/data_privacy/).