Project HealthDesign:

Rethinking the Power and Potential of Personal Health Records

The Need to Know: Addressing Concerns about Privacy and Personal Health Records

New PHR Approaches Require New Views of Privacy and Related Policies

Concern about patient privacy and confidentiality is as old as the practice of medicine itself. It is central to determining how medical providers and other institutions keep records on patients. By its nature, health care is very personal, and patients have always told doctors things they would prefer that others not know. The desire to protect privacy is in part an outgrowth of a basic human desire to live free of intrusion, judgment and prejudice.

Attention to privacy certainly predates the development of electronic recordkeeping. However, the advent of new technologies that enable collection and dissemination of large amounts of data at the push of a button—now common in today's world—necessitates an expanded view of what constitutes privacy.

Indeed, as personal information increasingly flows in bits and bytes, the need to use secure technologies and establish appropriate privacy practices goes far beyond the scope of exchanging information between health care facilities, insurers and other entities. With the emergence of personal health records (PHRs) and the fact that consumers increasingly play a more active role in their health, privacy considerations must now extend well beyond the standard types of medical information collected by providers (e.g., medication history, blood pressure) to include any information that factors into a person's health (e.g., sleep patterns, variations in pain levels).

An Expanded View of Privacy

Many clinicians, technology vendors, policy leaders, consumer groups, health researchers and health care advocates are promoting the adoption of PHRs as powerful tools that have the potential to revolutionize health and health care. When designed to meet patients' needs and fit into their lives, PHRs can help people make substantial and meaningful improvements in their health. If this potential is realized on a wide scale, the ripple effects of PHRs could be seen across America's health care system through greater efficiency, better quality, lower costs and more patient-centered care.

But as health data become more accessible and patients are empowered to manage their personal health information, many policy makers and

consumer advocates warn that the information contained in PHRs could be accessed by people that patients didn't authorize, improperly used by insurers or employers, abused by marketers or otherwise mishandled.

Raising these topics often results in a debate that pits privacy and consumer control against the ability of consumers and other parties to access their health information.

In order for PHRs to be effective and realize their potential, many experts believe that privacy cannot be synonymous with absolute confidentiality. Instead, these experts believe the notion of privacy should be expanded to incorporate some consideration of patient choice about what types of information can be shared, and with whom.

"In this modern world, what most people are talking about when they reference medical privacy is their discretionary right to decide who has access to their health information," says Stephen Downs, S.M., senior program officer and deputy director of the Health Group at the Robert Wood Johnson Foundation (RWJF). Along with the California HealthCare Foundation, RWJF is supporting *Project HealthDesign,* a national program to design next-generation PHR systems.

The project enlists technology designers, privacy experts, patients and others to explore new approaches to help people use their health information in practical ways. It encourages technology firms to build tailored, yet interoperable, PHR applications that operate on a common platform and meet patients' specific needs—including the need for privacy.

"Looking at this question through the lens of protecting privacy can lead you to solutions that elevate security at the cost of sacrificing greater utility," Downs says. "But there's a balance to be struck—if you look at it from the perspective of promoting individual control, you recognize that in addition to privacy, the ability to use the information effectively and the ability to share it are also very important."

Patients View Privacy As Having a Say in Who Sees Their Information

Experts say good information is central to good health care, and PHRs exist in part to enable the seamless and timely transfer of good information. It's a concept with which many Americans are comfortable. A 2006 survey commissioned by the Markle Foundation found that 97 percent of Americans think it's important for their clinicians to be able to access all of their records in order to provide the best care. Three-quarters of Americans are willing to share de-identified personal information to help public health officials monitor diseases and improve health research.

The nine teams supported by *Project HealthDesign* are identifying and incorporating patient preferences into their PHR applications. For many, this has meant learning more about how consumers view privacy.

"Managing privacy is a very hard thing for individuals to do, so designing technology that manages privacy is equally hard," says Patricia Flatley Brennan, R.N., Ph.D., professor of Nursing and Industrial Engineering at the University of Wisconsin-Madison and director of *Project HealthDesign.* "In a technological age, privacy often comes with technical choices and consequences, so we wanted to engage the technology community in the privacy debate very early on."

Project HealthDesign teams have found that while confidentiality is important to end users, they are often willing to share personal information in exchange for specific benefits and functions—assuming they are the ones empowered to grant

access to their health information and determine the level of access that others have to their information.

"Many Americans are used to sharing private information electronically in order to gain efficiencies that help them in their everyday life," Downs says. "Online banking and bill paying are perfect examples of this trade-off. Patients are not saying that their health information is so private that it can't be shared. They are saying that only *they* can make those decisions. That's how they view privacy."

Project HealthDesign Teams Learn from End Users

Several of the *Project HealthDesign* teams are actively exploring consumer attitudes about pri-

Privacy and Next Generation-PHRs

By offering an expanded view of PHRs, *Project HealthDesign* raises additional policy questions. In this expanded view, which the program often refers to as "next-generation PHRs," the service that maintains someone's personal health information provides a platform upon which many independent technology developers can build a broad range of tools. For example, a next-generation PHR service might maintain a person's list of current medications, but many different vendors might offer reminder systems that draw upon that medication information to send prompts or alerts that help people adhere to their medication schedules.

This model of PHR systems requires the services that store personal health information to publish application programming interface (API) specifications so that independent developers can build tools that work with the service. Doing so then raises questions of how to provide such access to personal health information through many potential intermediaries. To continue the medication example, the PHR service that maintains the medication list would receive requests for the medication list from a third-party vendor on behalf of the consumer. Policies that put strict restrictions on how PHR service providers protect data might limit the possibilities for third-party developers and thus stifle innovation, while policies that do not adequately protect the consumer from the risks associated with multiple "handoffs" of their information could discourage consumer adoption.

Whereas traditional PHRs have focused primarily on health information—such as diagnoses, medications, and lab results—that are generated through interaction with the health care system, *Project HealthDesign* grantees are looking at information that consumers generate in the course of their daily lives. Observations on diet, physical activity, pain, sleep patterns and medications taken, among other variables, provide valuable information that can be used to: provide people with direct feedback on day-to-day health behaviors; offer clinicians better understanding of their patients' health; and, through research studies, lead to new insights.

Including such user-generated information in a PHR service raises new policy questions, including:

- How is health information collected by patients treated differently than medical record information under current regulations? Is it adequately protected?
- Does an individual lose control over this information once she shares it with a health care provider? If so, does this create a significant disincentive to share the information?

vacy as they design novel PHR applications that people can use to better manage their health on a daily basis.

A team at the University of Washington School of Medicine led focus groups with adults who have diabetes to shape the design of its PHR application. The team is developing a system that enables patients to use cell phones to capture and wirelessly upload information—such as blood glucose levels—into their PHR and share it with their health care providers.

"Our application will allow people to share some of the information in their PHR with physicians, but not necessarily all of it," says Jim Tufano, a doctoral candidate in Biomedical and Health Informatics. "They liked the idea that they can

PERSPECTIVES:

Society has an Ethical Responsibility to Protect Patients' Privacy Rights

By Kenneth W. Goodman, Ph.D.

It is good and powerful and wholesome that privacy—a value first articulated when patient records were kept on papyrus scrolls—is still a value we champion now that patient information is digitized, collected, stored, shared and analyzed by intelligent machines. There are several lessons here—lessons for patients, clinicians, legislators and policymakers as personal health records and other evolving technologies place more of this sensitive information directly under patient control.

Privacy has never been a courtesy, grudgingly extended to people who were embarrassed by infirmity. Neither is its protection a legal abstraction, invented by legislators to placate those who have come to be called "privacy advocates" (who isn't?). And it is not an academic exercise, savored and pawed over by boffins in search of juicy dilemmas.

Privacy is perhaps best thought of as a human right enjoyed when people decide who can learn about them, and what those chosen can learn. That is, I—and you—get to decide who finds out if we have liver disease, schizophrenia, HIV or a boo-boo on a big toe. We do not give up that right when we tell our doctors and nurses what ails us, or ask them to find out.

There are several reasons for this. (Reasons are essential in ethics if we are to handle the tough cases as well as the easy ones.) One reason, as above, is that those who enjoy a right ought not need to convince others to protect it. Imagine if every journalist or parishioner had constantly to make the case that she ought to be able to write or worship what she wanted; or that every child (or parent) had always to prevail in debate over child labor or sexual exploitation. Similarly, we should not have to argue with clinicians or hospital administrators or entreat them to protect our privacy rights. That is society's job. Here, we do need the help of legislators and policymakers, but the right was there before they were.

PERSPECTIVES *continued*

Another reason for patient control of health information is that it enhances the quality of care. If I do not trust my doctor or nurse to safeguard my information I am apt to deceive him, and thereby frustrate the diagnostic and therapeutic processes.

We ought not touch people who do not want to be touched; we ought not confine people for no good reason; and we ought not acquire others' health information when they do not want us to.

Now, it is easy to misunderstand the job of ethics as consisting solely in issuing warnings and stipulating prohibitions and duties. But it is no such thing. Ethics, a branch of philosophy, has the task of analyzing and vetting arguments about values, intentions and right actions. Applied ethics guides clinicians and lawyers and scientists and bankers and legislators. At the nexus of ethics and policymaking, the job is to offer, rebut, improve and otherwise fine-tune arguments to ensure that society arrives at the best possible solution.

New technologies are a rich source of ethical challenges. It might be that use of a particular tool or gadget or device is inappropriate—or that *failure* to use the device is blameworthy. Personal health records have engendered great excitement because of their potential to improve patient care. So, to the extent that PHRs can thus improve care, it would be a mistake not to explore and expand their use.

PHRs raise distinctive privacy and other ethical issues, in part by virtue of the extent to which patients acquire greater-than-customary control over the very devices that store their information. We have the collective task of using the tools of ethics to identify and propose solutions to address these challenges. From clinic policy to federal law, ethics must be included in the processes that will govern use of personal health records—and then given the assignment of educating institutions and users about how to "ethically optimize" PHRs' various uses and applications.

By including an ethics component at the outset, *Project HealthDesign* is sending the message that applied ethics is a vital partner in the conception and fledging of an exciting new technology. Indeed, failure to include such a partner would arguably be a mistake every bit as serious as the failure to explore and develop PHR technology in the first place.

Kenneth Goodman is the founder and director of the University of Miami's Bioethics Program and associate professor in its School of Medicine. Goodman leads a team at the university providing consulting and educational support for Project HealthDesign *on the ethical, legal and social implications (ELSI) of health information technology and data sharing. The university offers a comprehensive online resource on privacy and health data protection, available at http://privacy.med.miami.edu.*

Ensuring the privacy of patient information and gaining an early understanding of the ELSI issues associated with the next generation of PHR systems are key objectives guiding the efforts of Project HealthDesign.

share part of their PHR with some people and other parts with other people. There are components of the PHR, for example, that they may want to share just with their nutritionist or just with other people who have diabetes. It doesn't have to be all or nothing, and they can control who sees what."

Tufano says his team's research showed a strong consumer preference against any information in a PHR being used without the patient's specific consent, even if data were de-identified.

"People know that medical researchers often need person-specific data to aggregate and analyze in order to draw valid conclusions. But even if their identity is totally removed from these records, the people we spoke with want to control whether their data are used for research purposes," Tufano said. "What I heard loud and clear was, 'This is my information and I may choose to share it with my peers or health providers, but I don't want it used for medical research unless I say so. And I certainly don't want drug companies to use it to target me for marketing or advertising.'"

A team at the Art Center College of Design in Pasadena, Calif., similarly is exploring ways to help adolescents with chronic illness more independently manage their health as they transition to adulthood. The teens want technological tools to help share information.

"These are kids who have grown up with Facebook, MySpace and YouTube, so they're comfortable putting all sorts of what we may consider very personal information about themselves on the Internet," says Sean Donahue, a research assistant at the Art Center. "That doesn't mean they don't expect a level of privacy. They may give 80 people access to their 'private' page, but they control who those 80 people are. That's very important to them."

"They also don't see controlling access to their medical information as posing a technology challenge. The privacy controls they expect from a PHR are similar to the privacy controls they get from Facebook. The great challenge for them is to learn to share personal information with a physician in order to better manage their condition."

An issue moving to the forefront

Even as the notion of digitized information was still emerging, policymakers envisioned the potential for misuse. In 1973, Casper W. Weinberger, then secretary of the federal Department of Health, Education, and Welfare, wrote, "It is important to be aware…that the computer…may have some consequences for American society that we would prefer not to have thrust upon us without warning. Not the least of these is the danger that some record keeping applications of computers will appear in retrospect to have been oversimplified solutions to complex problems and that their victims will be some of our most disadvantaged citizens."

Three-and-a-half decades later, this issue is at the forefront of U.S. health policy debates. The challenge: how to ensure that personal information maintained on a PHR is kept away from unintended eyes (and databases), while making sure that it is simultaneously—and easily—made available to those who need it and have been granted access to it.

Questions for Policymakers

Unfortunately—and even though the concept is ancient—privacy is not always clearly understood, and the term itself often is misused. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided a much-needed federal privacy law, and many state laws actually go beyond HIPAA in their efforts to protect sensitive health information. But HIPAA and most state laws come

across as largely provider-centric, defining privacy more in terms of institutional responsibility (e.g., HIPAA regulations apply to certain types of institutions, or "covered entities, and specify what they may or may not do with protected health information) rather than of individual rights.

"When it comes to PHRs and privacy, the law leaves us with a rather murky picture," says Brennan. "It's complicated. For instance, what happens to non-traditional health information that patients might collect in a PHR, such as their diet and exercise routines or how much they drink or smoke? It is critical to collect these daily observations in PHRs if we want to create applications that truly help patients take control of their health, but we also need to protect this type of data from being misused."

One of the central issues for consideration with any PHR application is the extent to which consumers have the ability to control access to their information. Some of the questions that policymakers, technology designers and consumers must address include:

- Can clinicians who have been given explicit access to PHR data by their patients share those data with others? If so, under what circumstances?

- Can some—but not all—of the information in a PHR be made available to a primary clinician or specialist?

- To what extent should family members or other members of one's care team (e.g., home health workers, school nurses and teachers, neighbors, etc.) be granted access to information stored on a PHR? Do special issues arise for dealing with these proxies?

- Who, if anyone, should have access to de-identified patient data for uses other than direct patient care (e.g., for biomedical research or public health)? Should patients be able to opt in or opt out of data use for broader public health purposes?

- Are existing data use notice and disclosure practices sufficient?

- What happens when sensitive health information is handled not just by those in the health care industry—hospitals, medical providers, employers or insurers—but also by non-traditional entrants in the PHR marketplace such as Microsoft or Google?

- Should HIPAA regulators expand their definition of what constitutes a covered entity?

Moreover, questions tied to PHRs and consumer privacy can not be debated solely in theoretical terms; the search for new solutions will necessarily be constrained by practical considerations. New technology developments may push our understanding of what is technically feasible, but the reality is that consumers will likely resist adopting tools and applications that are too unwieldy or burdensome when it comes to managing their data.

These questions are attracting the attention of policymakers at both the federal and state level. Several bills pending in Congress would expand federal administration of health privacy. These include the bipartisan "Wired for Health Care Quality Act" (S. 1693), which would broaden the definition of a covered entity under HIPAA and identify circumstances under which individuals should be notified if their identifiable health information is wrongly disclosed;

and the "Health Information Privacy and Security Act" (S. 1814), which seeks to protect health information privacy while still promoting the use of non-identifiable health information for research.

Providing Direction

Robert Kolodner, M.D., oversees the Bush Administration's efforts to encourage Americans to embrace an interoperable medical record system. As national coordinator for Health Information Technology at the U.S. Department of Health and Human Services (HHS), Kolodner's charge includes promoting the use of PHRs and ensuring that privacy and security issues are properly addressed. Additionally, the American Health Information Community, a federal advisory group that was created to counsel the government on such matters, has convened a workgroup that is forming recommendations regarding the protection of personal health information.

Questions remain, however, as to whether these efforts are sufficient to address the aspects of the personal health record—in contrast to the professionally generated electronic medical record. A recent U.S. Government Accountability Office report was critical of privacy oversight and recommended that HHS "define and implement an overall privacy approach that identifies milestones for integrating the outcomes of its initiatives, ensures that key privacy principles are fully addressed, and addresses challenges associated with the nationwide exchange of health information."

Many policymakers, foundations, software vendors, informatics experts, consumer groups, providers, insurers, medical researchers, privacy advocates and others are also grappling with these issues. The Health Privacy Project (www.healthprivacy.org), which advocates for greater protection of health information, will make recommendations later this year about guidelines for PHR privacy. The Markle Foundation's *Connecting for Health* program (www.connectingforhealth.org) will release guidelines in late 2007 that identify rules that organizations should follow with respect to PHRs and privacy.

"This widespread interest in health information and privacy is important," says Downs. "I don't think any one organization or person thinks they have the answer. At some level we all have the same goal: we want people to embrace this technology because we truly believe that PHRs can be designed to help people manage their health in ways that fit into the flow of their daily lives. If implemented to their full potential, PHR systems will empower consumers, increase interaction between patients and doctors, improve the quality of care and help people live healthier lives. But we've got to get the privacy issues settled or it will never work."

For More Information

Project HealthDesign is funded by the Robert Wood Johnson Foundation and the California HealthCare Foundation. The University of Wisconsin-Madison serves as the National Program Office (NPO) and provides direction and technical assistance for the initiative. For more information and to sign up for program updates, please visit www.projecthealthdesign.org

Project HealthDesign

Patricia Flatley Brennan, RN, PhD
National Program Director
University of Wisconsin-Madison School of Nursing
600 Highland Avenue, CSC H6/297
Madison, WI 53792
info@projecthealthdesign.org
www.projecthealthdesign.org