



GEORGETOWN UNIVERSITY

Institute for Health Care Research and Policy

Testimony before the

National Committee on Vital and Health Statistics
National Health Information Infrastructure Workgroup
Hearings on Health and the National Information Infrastructure
and the NHII Personal Health Dimension

Joy L. Pritts, J.D.
Assistant Research Professor

January 22, 2003

www.georgetown.edu/research/ihcrp

Mr. Chairman, Members and Staff of the National Committee on Vital and Health Statistics, National Health Information Infrastructure Workgroup on:

Thank you for the opportunity to testify before you today on privacy issues related to the personal health record aspect of the National Health Information Infrastructure. I am Joy Pritts, an Assistant Research Professor at Georgetown University's Institute for Health Care Research and Policy and former senior counsel for the Health Privacy Project. In my position at Georgetown, I conduct research and analysis on a range of health privacy issues. My focus has been state and federal health privacy laws, and particularly how they protect health care consumers. My recent publications include: *The State of Health Privacy*, a compilation of major state health privacy statutes, *Implementing the Federal Health Privacy Rule in California*, and "Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule," *Yale Journal of Health Policy, Law, and Ethics* (Spring 2002).

I. INTRODUCTION

As envisioned by this committee, the National Health Information Infrastructure encompasses three dimensions: the healthcare provider dimension (which addresses the needs of healthcare providers for complete and accurate patient and practice data), the population health dimension (geared towards protecting and promoting the health of the community), and the personal health dimension, which supports individuals in managing their own wellness and healthcare decisionmaking. The personal health record, which we are discussing today, is one of the key applications of the personal health dimension.

Currently, there are a number of different types of organizations that offer "personal health records" today. They include commercial vendors, health care providers, insurers, employers, and patient advocacy groups. By no means are the characteristics of these personal health records uniform. However, they generally have at least the following key elements:

- Internet based
- Accessible to the patient
- Allow patient to input health data
- Give patient control of who may access their personal health
- Integrate or summarize personal health information from multiple sources

The potential benefits of such a personal health record are significant. Personal health records can further the developing role of patients as partners in their own health care. This type of record can provide access to key, accurate, up-to-date health information to patients and providers in a timely, concise fashion. Additionally, their use can improve the quality of care by reducing medical errors and duplicative procedures.

Yet, to make the personal health record a reality, a number of issues need to be addressed. From the perspective of health care consumers ensuring the privacy of these records is paramount. Some of the key privacy issues that are presented by the personal health record include:

- To what degree does the individual (or patient) control the personal health record?
 - Does the patient control input?
 - Do the patient have control over who else may access the information in the personal health record?
- What legal protections are afforded the personal health record?
- What are the security concerns raised by the personal health record?

My testimony today will address some of these key privacy concerns.

It is imperative to recognize that the nature and extent of these concerns varies widely with the entity maintaining the personal health record. For purposes of illustration, I will focus on privacy issues that arise with two categories of those who maintain personal health records: commercial ventures and health care providers.

II. COMMERCIAL VENDORS

A. PATIENT CONTROL

A number of commercial web sites offer some form of a personal health record. They allow a patient to enter personal data into a record that is maintained by the web site. The patient has the right to see and change the record as he or she sees fit. The patient also has the right to allow others to see the information. On some sites, they recommend that the patient print out their personal health record and take it to their doctor with them. Other sites are more interactive and allow the patient to designate certain providers who are able to review the record, and in some instances, add data to the record. They often provide access to the personal health record to health care providers in emergency circumstances, either through use of a PIN or other means of identifying the individual.

Prominently displayed on many of these web sites is the claim that the information will be kept “private and confidential” and that the patient controls who will have access to his health information. In fact, one of the big selling points for this type of personal health record is the apparent high level of control that patients will be able to exercise. The patient has full access to his or her own information in the record. Generally, it is that patient who controls what information is entered into the record. And it is the patient who has control over who else may access his personal health information.

It is somewhat misleading, however, to tout these personal health records as a means for patients to control their own health information. There is no doubt that this type of personal health record makes it easier for patients to provide information to or transfer health information between health care providers. And it is also true that patients can control who has *direct* access to their personal health records.

But once the patient permits any health care provider to access his personal health record, the patient has little control over the information—the health information will flow through the health care system with little, if any, input from the patient. For example, let’s assume a patient allows his primary care physician access to his personal health record that is maintained on a web site. Upon review, the physician will likely incorporate part, if not all, of the personal health

record into the medical record that the physician maintains on the patient. Now the information is part of the physician-maintained record, which is considered to be the physician's property under state law. Additionally, the information has now become "protected health information" under the Federal Health Privacy Regulations. At this point, even if the patient has some large dispute with the physician the patient cannot retrieve his health information. He cannot delete the information. At best, he can amend it. And he cannot prevent the physician from using and sharing it without his permission for the vast panoply of treatment, payment and health care operations purposes permitted under the Federal Health Privacy Regulations. Similarly, the information can be used for research and public health purposes without the patient's permission.

There are, of course, restrictions on using or sharing this information for non-health care related purposes. But many patients are interested in using a personal health record as a means of controlling their information *within* the health care system. It is highly unlikely that these expectations will be met once a patient permits the information in his personal health record to be accessed by a health care provider.

Thus, while a patient has a high degree of control over what information is entered into his personal health record, as a practical matter once the patient grants any provider access to this personal health record, the patient largely loses control over how the information may be used and who it will be shared with. While there may not be anything inherently wrong with this flow of information, patients need to be fully aware of it from the outset. Vague promises of "patient - centric records" and "privacy and confidentiality" do not adequately inform patients of how their health information will be used and shared with others.

B. LEGAL PROTECTIONS

In addition to concerns about the amount of control patients truly will be able to exert over their personal health records there are also serious issues surrounding the legal protections afforded these records when they are maintained by commercial vendors, particularly those that are Internet based. The primary federal law governing the use and disclosure of health information would be the Federal Health Privacy Regulations promulgated by the Department of Health and Human Services under HIPAA. However, it is quite likely that the Federal Health Privacy Regulations will not directly cover most of these web sites. The Federal Health Privacy Regulations directly regulate only health care providers who engage in certain transactions electronically, health plans, and health care clearinghouses. Most of the web sites that maintain personal health records do not fall in any of these categories.ⁱ

Similarly, most state health privacy laws do not apply to web sites that maintain personal health records. Overwhelmingly, state health privacy laws focus on health care providers and insurers, categories that do not encompass web sites that maintain personal health records.ⁱⁱ

Some degree of protection is provided by the Federal Trade Commission Act, which prescribes unfair acts affecting commerce. For instance, the FTC can bring an enforcement action against a web site that violates its own privacy policy.

But even the FTC may not be able to protect health information if a commercial vendor goes out of business. The circumstances surrounding Toysmart.com's bankruptcy present a prime example of the limited legal protection of "confidential" information when a commercial online vendor dissolves. Toysmart.com sold toys on the Internet and collected customers' addresses, buying habits, children's names and ages and other personal information. The company's posted privacy policy stated that its customers' personal information would never be shared with a third party. When the company filed for bankruptcy, it attempted to sell its most valuable asset -- its customer information. The FTC stepped in, challenged the sale, and reached an agreement with the company that would place restrictions on the sale of the information. However, that agreement was overturned by the bankruptcy court, which was more concerned with asset valuation and creditors' rights. Although there eventually was a satisfactory ending to this particular taleⁱⁱⁱ, it was not due to any formal legal protections.

The idea that the privacy of personal health records maintained by commercial web site vendors could be similarly threatened is not far-fetched. The Internet is a markedly volatile environment, and sites offering online personal health records come and go at a frightening pace. A recent survey originally identified 66 companies providing online personal health records, but by the end of the 12-month study only 16 still offered the service.^{iv}

This lack of legal protections for the privacy of health information maintained by commercial web site vendors is striking. Without these protections, it would be remiss to consider commercial vendors as viable components in the National Health Information Infrastructure.

III. HEALTH CARE PROVIDERS

Health care providers are also increasingly offering patients a form of "personal health records". Generally, they permit an individual to read their medical record, review test results, and submit health information. Personal health records maintained by health care providers more accurately may be seen as interactive electronic medical records and present their own set of privacy issues.

A. PATIENT CONTROL

By allowing patients to see and amend their medical information, this type of personal health record clearly affords patients some degree of control over their health information. The extent of patient control is less than that afforded by commercial vendors.

It is self-evident that patients have less control over the content of a personal health record maintained by a health care provider, where the provider enters the information, than the content of a personal health record maintained by a commercial vendor, where the patient enters the data. Additionally, the patient may also have less access to health information maintained by a health care provider. Although providers are required to allow patients access to their health information under the Federal Health Privacy Regulations, providers are also permitted to deny access in certain circumstances, particularly when they believe that access would endanger the life or physical safety of the patient or another person.

Patients also have less control over who else has access to personal health records maintained by providers. It is likely that any health care provider who interacts with the patient will have access to such a record without the patient's express authorization.

Overall, however, there should be less of an issue about unmet expectations with provider controlled information. The fact that the date is primarily entered by the provider (or group of providers) and is maintained by the provider should serve as a signal that the patient does not have primary control over the record. The opportunity for a disconnect between patient expectations and reality in this circumstances still exists, however., because most health care consumers currently believe (inaccurately) that they, not the provider, own their medical record.

B. LEGAL PROTECTIONS

Health care providers maintaining personal health records generally will be covered by the Federal Health Privacy Regulations. As covered entities, they will be required to furnish patients access to their own health information and will be subject to the use and disclosure restrictions of the regulations.

It is not clear exactly how the personal health record will be implemented within the framework of the Federal Health Privacy Regulations' patient access requirements. Will the provider consider a patient's logging onto the site as a formal request for access to personal health information under the Federal Health Privacy Regulations? Will the online personal health record routinely provide patients access to all their health information, or only certain components? If the online version is only a partial record, providers will need to ensure that there is a clear mechanism for patients to request their entire medical record and that patients are aware of that procedure.

With respect to uses and disclosures, health information maintained by health care providers will be afforded the protection of the Federal Health Privacy Regulations. Although providers will be able to use and share the information freely for treatment, payment, and health care purposes, they will be required to allow patients to request restricted use and disclosure in these areas. Providers will also be required to obtain patient authorization to use or disclose their health information for many non-health care related purposes. The regulations also prohibit the sale of this information to third parties without patients' permission unless the sale would be to another entity that is covered by the regulations. Thus, the issues presented by Toysmart.com should not be applicable to personal health records maintained by health care providers.

Even with these protections, however, some health care consumers will be dismayed at the minimal level of control they have over the flow of their health information within the health care system.

C. WHERE DOES THE MINIMUM DATA SET FIT IN?

ⁱ Some web sites might be covered by the Federal Health Privacy Regulations because they engage in other functions that ARE covered, such as being a health care clearinghouse. However, it probably will be difficult for health care consumers to discern whether a web site is covered by HIPAA.

ⁱⁱ A notable exception is California's Confidentiality of Medical Information Act, under which a web site that maintains personal health records for patients is required to maintain the same degree of confidentiality as a provider. See Cal. Civ. Code § 56.06.

ⁱⁱⁱ The Disney Company, which had invested in Toysmart.com eventually bought the list and destroyed it.

^{iv} Schneider, JH Online Personal Medical Records: Are They Reliable for Acute/Critical Care?, *Critical Care Med* 2001; 9(8, Suppl) N196-N201.