A Pilot Study: Patients' Perceptions About the Privacy of Their Medical Records

By

Linda Goodwin, RN, C, PhD, Karen Courtney RN, MSN, J. David Kirby, Mary Ann Iannacchione, RN,

and Tina Manley, MSN, RN

Abstract

A descriptive pilot study was designed to explore patients' perceptions of privacy and trust within the context of data sharing and their personal health information. Results (n=92) found that patients were generally unaware, misinformed, or confused about data and personal health information practices and believed that there was less data sharing than is routinely practiced in health care. Nearly 85% of patients studied reported "total" to "pretty good" levels of trust in their health care system. Less than 5% indicated they "didn't care much" about personal health information privacy. Prior problems with privacy of their medical records were reported by 13% of the subjects. With enactment of The Health Insurance Portability and Accountability Act of 1996 PL 104-191 (CMS, 2002), health care organizations have federally mandated privacy regulations. Improving patient and provider education about data storage, sharing, and protection will evolve as HIPAA regulations are implemented. However, improved education carries an additional risk of eroding patient trust in the health care system as consumers become more aware of widespread data sharing in health care.

Keywords

Privacy, Patient Trust, Personal Health Information, Patient Records, Data Sharing

A Pilot Study: Patients' Perceptions About the Privacy of Their Medical Records

Background and Significance

Privacy, *confidentiality*, and *security* are often used interchangeably to refer to the protection of personal health information. According to the Committee on Maintaining Privacy and Security

in Health Care Applications of the National Information Infrastructure (National Research Council, 1997) *privacy* refers to an individual's desire to limit the disclosure of personal information while *confidentiality* refers to a condition in which information is shared or released in a controlled manner. Physicians and nurses, for example, have professional codes of ethics which include confidentiality. *Security* consists of measures that organizations implement to protect information, and includes technology as well as policies and procedures for safeguarding patient data.

The proliferation of computerized patient records increases the privacy risk of patients and confidentiality obligations for health care providers. Aggregating data into computerized databases and distributed computing networks increases both the risk and the likelihood that information will be improperly disclosed (Office of Technology Assessment, 1993). Most patient privacy violations have been, and will continue to be, made by persons who have legitimate access to a patient's data (Kibbe & Bard, 1997). But privacy violations did not begin with computers. Within health care organizations, computerized patient records are vulnerable to both authorized users who misuse their privileges (such as browsing through all patient records) and outsiders who are not authorized to use the information systems, but break in with malicious intent.

Many people worry about the potential consequences of privacy breaches; indeed, nearly 75% of our nations' citizens are at least somewhat concerned that computerized records will have a negative effect on their privacy (Shalala, 1997). Widespread public mistrust may cause patients to fail (or refuse) to disclose accurate and vital information to their health care providers (Goold & Klipp, 2002). In addition, patients may avoid genetic and other diagnostic testing, and may

refuse to participate in clinical research that could have personal benefits for patients and increase the progress of medical care (Rothenberg & Terry, 2002). A recent survey found that one in six people is "privacy-protective" when utilizing health care; patients give inaccurate or incomplete information in their medical histories, ask their physician to not record embarrassing information in their records, change physicians frequently, refuse to seek treatment, or pay out of pocket in an effort to protect their privacy (Pritts, et al, 1999). Lester (2001) reports that where privacy is concerned, 12% of the public is unconcerned about privacy and don't worry about how their personal information might be used, while 63% are willing to balance potential benefits and threats of sharing their personal information, and 25% reject any benefits that require release of their personal information.

Etzioni (2001) describes four different models for the analysis of patient privacy. A *constitutional rights model* views privacy as a constitutional right that cannot be sold, given away, or traded. A property rights model views privacy as a property right than can be given away, sold or traded. A *liberal* model views privacy as something for which the government can establish rules to protect use of private information. And a *trust* model views health care providers as trustworthy for using the information only for patient benefit. A rapid high-level analysis in health care will find that both the constitutional and property rights models have been rejected in favor of a trust model (Kirby, 2002). This trust model is no longer able to guarantee that information will be shared only for patient benefit. Health Insurance Portability and Accountability (CMS, 20002) regulations fall into the liberal model, and their impact on both privacy practices on the part of health care providers and organizations, as well as on the public trust, are yet to be determined.

While computers do, in fact, increase the risk for sharing personal health information (Office of Technology Assessment, 1993), technology also holds many solutions that may actually improve the security of patient data. Biometric authentication, for example, uses a person's voice, retinal pattern, fingerprint, or face recognition to assure that the person has legitimate access to the data (Liu & Silverman, 2001). Firewalls block unauthorized access to data on many networks (National Institute of Standards and Technology, 2002). Audit trails track every access to the data, and increasingly are used to notify a security officer of misuse by authorized users and attempts to access data by unauthorized users (Office of Technology Assessment, 1993). Encryption offers new levels of security that are already being used in many research studies (National Institute of Standards and Technology, 1996). The patient's identity can be encrypted and the data provided to a researcher who cannot identify the individuals being studied; in the event of a problem, the researcher can contact the office where encryption was performed and, with Institutional Review Board (IRB) approval, the data can be de-encrypted to identify the patient if that is in the patient's best interest. Smart cards look like credit cards and can store a person's health information that they carry around in their wallet; the patient controls who has access to the information (Office of Technology Assessment, 1993). Privacy issues in health care involve more policy and procedural issues than those related to technology (Association of American Medical Colleges, 2001; Callas & Brockmeier, 2001; Craig, 2001).

Historically only 10% of the nation’s health care transactions were electronic, but with enactment of HIPAA 1996 (CMS, 2002) legislation which mandated Transactions and Codes (August, 2000) and Privacy (December, 2000), health care organizations using electronic claims transactions must comply with federally mandated electronic transaction statutes. Recent congressional action allowed an extension, for those who apply, to the compliance date for

Transactions and Codes until October 16, 2003 but compliance for Privacy regulations remains at April 14, 2003. Duke University Health System has been on the leading edge of HIPAA compliance efforts. One component of Duke's compliance plan is patient education. The Duke University Health System website for patients and visitors (http://www.dukehealth.org/patients_visitors/) includes links to a "patient's bill of rights" and confidentiality information for patients and potential patients. In most HIPAA compliance literature however efforts are directed to education of health care providers and administrators without addressing patient educational needs (Association of American Medical Colleges, 2001; Callas & Brockmeier, 2001; Craig, 2001). Of interest is whether or not web references and posted material in waiting rooms is sufficient for educating patients.

When asked if they used a computer to access the Internet, results that found 85.9% of the subjects responded that they were using computers to access the Internet. However, we do not know how patients perceive their privacy risks or whether patients are aware of the web-based information provided by the university on privacy and confidentiality. This pilot study was designed to explore three areas: awareness of information flow, awareness of current privacy policies and procedures and level of concern about medical information privacy.

Design and Procedures

Patients were asked to complete a brief and anonymous questionnaire that examined their awareness of the flow of their personal health information, as well as their perceptions of privacy and trust in relation to how their information is managed by the Duke University Health System. After IRB approval, patients had the study explained to them by a nurse who worked in one of the participating clinics; the nurse also screened patients for inclusion in the study, explained the study to each patient, and provided the questionnaire to those who volunteered to participate.

The questionnaire shown in Table 1 was developed for this pilot study and consisted of 12 questions with forced choice answers and space for additional comments. To assure patient privacy, there were no identifiers of any kind on the questionnaire and anonymity was assured. Patients could complete the questionnaire in approximately 5 minutes while they were waiting to be seen by their provider in the clinic; the completed questionnaires were placed in an envelope that subjects sealed and returned to the clinic nurse who collected, stored, and delivered them to the principal investigator. Upon return of the sealed envelope, subjects were given a printed copy of the health system's confidentiality statement (http://dukehealth.org/patients_visitors/confidentiality.asp).

Table 1: Questionnaire

	Question
1.	How would you describe the information you expect to give to clinic personnel today?
2.	How do you think your patient information is stored at Duke?
3.	Do you think it would be possible to take your patient/medical record home with you?
4.	Do you think it would be possible to get a copy of your patient/medical record?
5.	Have you read Duke's confidentiality information?
6.	Have you seen a patient bill of rights?
7.	Who do you think OWNS your personal health information?
8.	How much do you TRUST that your personal health information will remain private?
9.	How much do you CARE that your personal health information will remain private?
10.	When you leave the clinic today, where do you think the information you gave the registration clerks, clinic staff, nurses, and doctors might go?
11.	Have you experienced any problems in the past with privacy and your personal health information?
12.	Do you use a computer to access the Internet?

Results

Ninety-two participants in the study completed questionnaires with complete anonymity; subjects were patients in urology or perinatal outpatient clinics at Duke University over a one-month data collection period. Subjects who were over the age of 18, or parents who provided consent and information for pediatric patients, completed the anonymous questionnaire, placed it in a sealed envelope, and returned it to the clinic nurse. The study was based on an assumption

that protecting a patient's privacy remains a core value in health care. However, in an information age of pervasive data sharing and increasing computerization, the practices and procedures for actually accomplishing privacy protection become quite complex. This study found that patients were generally unaware, misinformed, or confused about data and information practices with regard to their personal data and health records and, generally, thought that there was less data sharing than is routinely practiced.

Information pertaining to an individual's medical condition makes up the medical record for that person, and keeping a patient's secrets private is a basic element of the Hippocratic Oath (written 400 BC, accessed 2002). In this pilot study, people felt strongly that details about them should not be divulged, although it is virtually impossible to practice medicine without sharing data and information with others. For example, insurance companies insist on access to the medical record in order to process claims for medical coverage; therefore, waiving of confidentiality is required to get insurance payments. As shown in Figure 1, almost half (48.9%, N=45) of the respondents stated that information given during a clinic visit was *extremely* personal and private, and 32.6% (30 individuals) considered that information *fairly* personal and private.

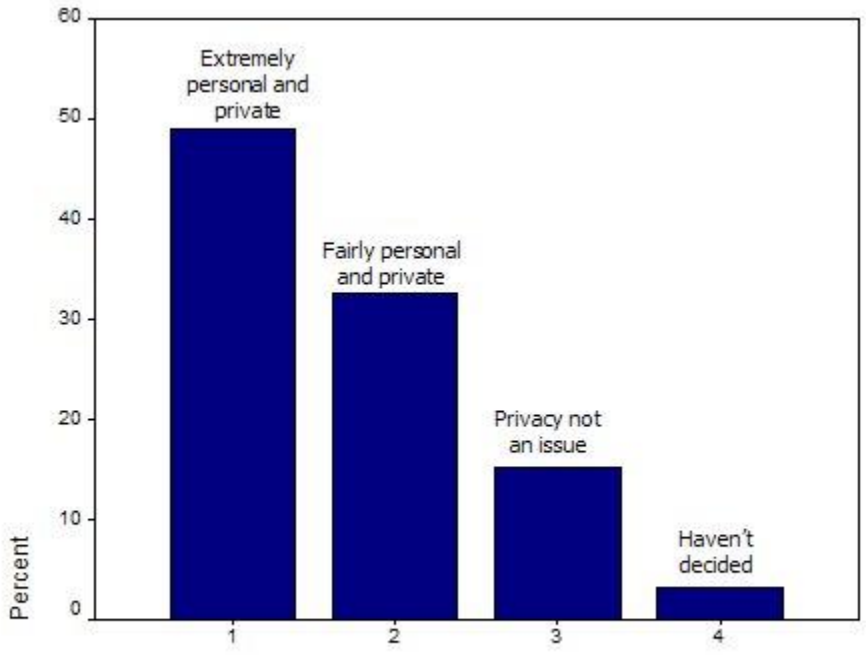

Figure 1: *How would you describe the information you expect to give to clinic personnel today?*

When a patient checks into a clinic prior to an appointment, a paper medical chart is usually available, having been pulled from the filing and storage area in the Medical Records Department. Often, a computer is a fixed item in the examination room, and is used along with a paper medical chart for recording patient health information. Paper charts have always been around, but with more and more exposure to computers in exam rooms, patients' may think that computers are replacing the paper method of keeping medical information. While paperless medical records have been a goal for decades, *very* few organizations have achieved that goal (Hammond, 2001). Table 2 provides participants' perceptions of where and how they believe their patient information is stored.

Table 2: *How do you think your patient information is stored at Duke?*

	% Yes	% No
On paper in the clinic	37.0	63.0
On computers in the clinic	56.5	43.5
On paper in the doctor's office	23.9	76.1
On computers in the doctor's office	34.8	65.2
On paper in the Medical Records department	44.6	55.4
On computers in the Medical Records department	60.9	39.1
Other (please list)	3.3	96.7

Well over half of the respondents thought their patient information was stored less on paper than in the computer. The majority thought their information was stored on computers either in the clinic or in Medical Records. One subject marked "other" and wrote in "hospital wide data base" reflecting an awareness of current health care information system trends. In reality most clinic patient records include both paper records that are stored in Medical Records and computerized components that are stored "in" Medical Records but are sometimes physically located with information system servers outside the Medical Records department. As Figure 1

indicates, the majority of subjects in this study indicated that they considered the information provided in their clinic visit as personal and private, yet their answers to this question indicate they did not know where the data were stored after they left the clinic. With HIPAA privacy compliance, health care organizations and providers have an obligation to improve the information they provide to patients with regard to data and information storage practices in a "Notice of Privacy" (U.S. Department of Health and Human Services, 2002).

One question asked patients about taking a medical record home, whereas a second question asked about taking a *copy* of the record home. Almost half of all participants (47.8%) accurately responded that they did not think they could take their medical record home with them. However, a large number were undecided (17.4%) about the question, perhaps reflecting the subtle differences between the two questions and 34.8% erroneously believed they could take their medical record home with them. The majority of respondents (89.1%) believed they could take a copy of their medical record home with them and only 2.2% felt they could not access a copy of their record. One subject commented, "Only if someone is there to explain to me in the office – I can see my chart".

Responses on ownership of personal health information were surprisingly divided; 47.8% or 44 respondents thought they owned their personal health information, and 52.2% or 48 people thought they did not. Interestingly, the vast majority of participants, 98.9%, (91 people) said that the place that paid their medical bills did *not* own that information. HMO and health insurance companies would do well to address this perception of medical information ownership. Table 3 provides the patient perspective on who owns a patient's personal health information.

Table 3: *Who do you think OWNS your personal health information?*

	% Yes	%No
The patient (me)	47.8	52.2
The doctor	9.8	90.2
The clinic or hospital	32.6	67.4
The place that pays my medical bills	1.1	98.9
Don't know	16.3	83.7
Other	2.2	97.8

HIPAA regulations clearly say that patients own their personal health information (U.S. Department of Health and Human Services, 2002). While this may seem obvious to patients, historical practices have empowered the organizations that collected the data, not the patient, to claim ownership. As more educated consumers of health care begin to claim ownership of their personal health data and information, new policies and practices will be required by health care organizations that have not previously operated in this paradigm. Indeed, the concept of patient ownership of their personal health information is a paradigm shift for health care enterprises and will require expensive systems-level change (Association of American Medical Colleges, 2001; Moynihan, 2001. It is perhaps not surprising that the American Hospital Association, the American Medical Association, and the health insurance industry have lobbied to have the HIPAA regulations delayed or repealed (Anonymous, 2001).

Prior to passage of HIPAA regulations, many health care organizations made efforts to inform patients of their rights. A patient's bill of rights is posted in both English and Spanish in the waiting rooms of each of the health system clinics and it is now provided as a small flyer on the counter at the registration desk when patients check in for their clinic visit. The subjects in this study were about evenly split between those who had and those who had not seen a patient bill of

rights. Table 4 shows patient responses with regard to a patient bill of rights and the Duke University Health System confidentiality statement (http://dukehealth.org/patients_visitors/confidentiality.asp).

Table 4: *Questions about patient bill of rights and confidentiality information.*

Pilot Study Research Question	*Yes*	*No*	*Don't Know*
Have you seen a patient bill of rights?	41.3%	43.5%	15.2%
Have you read Duke's confidentiality information?	42.4%	34.8%	22.8%

Less than half of those surveyed (42.4%) had read Duke's confidentiality statement. Confidentiality statements are posted for public access on Duke's web site, and are also posted as framed documents in each clinic yet over half of the subjects in this study either had not read it (34.8%) or did not know (22.8%) if they had read it. Patients come in contact with a multitude of forms and papers and reading a confidentiality statement may be considered a low priority; however, this is the document that describes what a patient can expect in regard to the storage and dissemination of personal health information. The importance of reading and understanding this information should therefore be emphasized. A printed confidentiality statement should be prominently displayed so that people can read it (Office of Technology Assessment, 1993). An educational campaign to increase awareness that a confidentiality statement exists may be necessary; staff members, by referring to the posted statement, then will have the opportunity to introduce the topic while the patient is in the clinic. Subjects in this study were provided with a copy of the web-enabled confidentiality statement, along with the website address where they could access the information at any time. Careful stewardship of confidentiality obligations on the part of the health care organization provides a foundation for patients to trust health care providers with their personal health information.

Trust includes a conviction that confidentiality will be maintained; i.e., information will be shared or released only in a controlled manner. An additional factor in trust is the belief that security measures are used to protect that information. When asked how much they trusted that their personal information would remain private, 21 of these subjects (22.8%) reported total trust, and 57 (62%) had a pretty good level of trust.

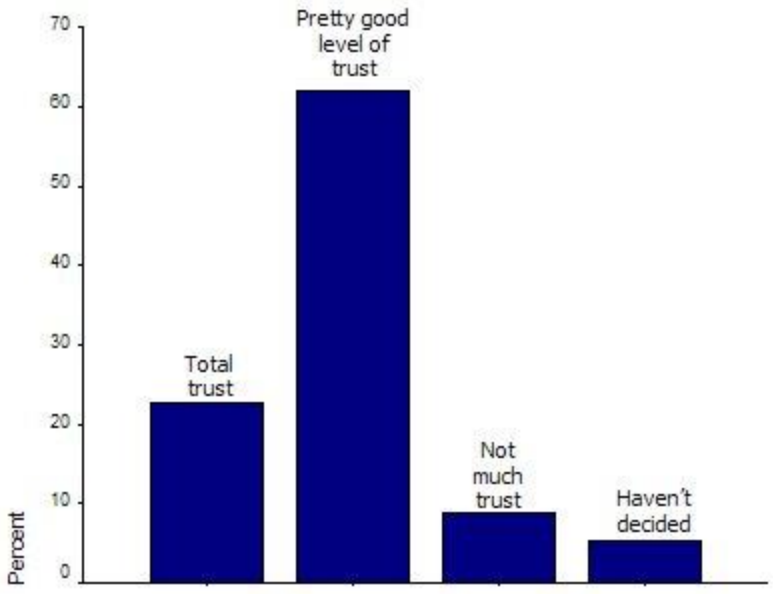

***Figure 2**: How much do you trust that your personal health information will remain private?*

It seems possible that patients' high levels of trust are at least partially the result of their lack of awareness of widespread sharing of their data throughout a complex health care system. For example, medical information may be passed on to direct marketers or it may end up in the databanks of businesses that sell products related to a test. One case in point, the Medical Information Bureau (MIB, 2002) was established in 1902 to help prevent insurance fraud and is a central database of medical information. Approximately 15 million Americans and Canadians are on file in the MIB's computers. Over 750 insurance firms use the medical risk clearinghouse services of the MIB, primarily to obtain information about life insurance policy applicants. The decision on whether to insure an individual is not supposed to be based solely on the MIB report, and the MIB does not have a file on everyone. Patients are generally unaware that the MIB exists, but if a patient's medical information is on file, that person can obtain information by writing to the Medical Information Bureau.

As noted previously, privacy refers to an individual's desire to limit the disclosure of personal information. When participants (n=92) in this study were asked how much they cared that their personal health information would remain private, 80% said they cared "a lot" about privacy, while less than 5% of participants did not care about privacy or were undecided. These results are similar to a 1995 Harris Poll (cited in Voran, 1998), which showed that 84 % of Americans were concerned about threats to privacy.

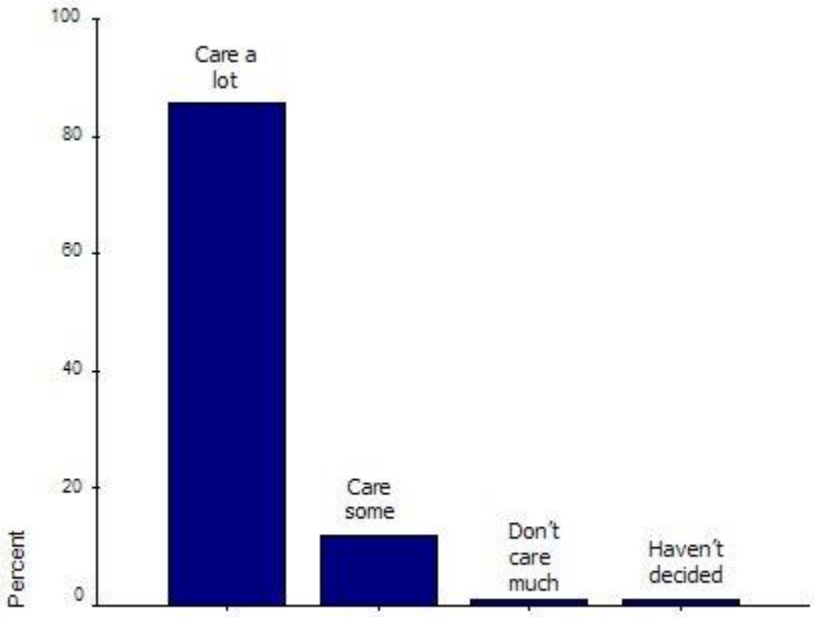

Figure 3: *How much do you care that your personal health information will remain private?*

Patients were asked, "When you leave the clinic today, where do you think the information you gave the registration clerks, clinic staff, nurses, and doctors might go?" Answers reflected a mixture of confusion, lack of awareness, and misperceptions. The top four responses were medical records (89.1%), doctor's office (63.0%), insurance company (59.8%) and Patient Accounts and Billing Departments (52.2%). Over half thought their information would go to these destinations. Interestingly, respondents did not seem to think their information would go to

ancillary services such as pharmacy (93.5% No), physical therapy (100.0% No), radiology (98.9% No), respiratory therapy (98.9% No), social services (100.0%), case management (83.7%) or laboratory (87%).

Clinic patients accurately thought (100%) that information would not go to the gift shop or housekeeping areas. They made the same assumption about Social Services, yet based on typical demographics in these clinics; it is highly likely that Social Services referrals were made for some patients. In general, participants' responses indicated lack of awareness of information sharing for quality improvement, research, government reporting and billing, accreditation requirements, case management, credit and Medical Information Bureau reporting, and administrative uses.

Almost half of the respondents said that the information given during the clinic visit was extremely personal; the gap between patients' privacy values and their lack of awareness about where all their personal information was going raises questions. The National Research Council (2001) reports that personally identifiable health information is frequently shared with consulting physicians, managed care organizations, health insurance companies, life insurance companies, self-insured employers, pharmacists, pharmacy benefits managers, clinical laboratories, accrediting organizations, state and federal statistical agencies, and medical information bureaus. As patients become more aware of this widespread data sharing, and as increasing numbers of patients are harmed through this activity, public trust in the health care system has come into question (Pritts, et. al., 1999). Patients are not aware that approximately 150 people look at their personal health data, and many believe that only their primary care providers, and perhaps their assistants, have access to a patient's data (Pfizer, 2001). In general, patient

awareness has not caught up with the fact that they are dealing with large health care business enterprises, not just their local primary care provider.

Another question asked patients if they had experienced any problems in the past with privacy of their personal health information. The overwhelming majority (87%) had not experienced any problems in the past. Considering their low level of awareness, however, one wonders if there really had been no problems, or whether subjects were not aware of potential or existing problems. Many forms of privacy abuse may not be apparent to the patient. One wonders if we should be shocked or pleased that 13% of patients in this pilot study had privacy problems of sufficient severity that they became aware of them.

Clinical Implications

Given the large number of patients in this study who were unsure whether they had read a patient bill of rights, it is important to determine the reading and literacy levels of the patient populations being served, and match signage (or verbal explanations) to their needs and abilities. Vulnerable populations are not always able to read and comprehend 8th grade English patient education materials, and it is important to be sensitive to this issue in the clinical setting.

Health information is collected and used in many areas, including worker's compensation forms, live birth statistics, Medicaid eligibility, cancer death rates, and listing of health restrictions on driver's license applications. Sharing and reuse of data raise concerns about patient identification and the need to monitor the flow of information. The need to educate patients about use and re-use of their personal data needs to be honest and balanced with education about the benefits of data sharing as well as the risks.

HIPAA will require privacy, confidentiality, and security initiatives throughout all health care systems. Since the Joint Commission on Accreditation in Health Care Organizations (JCAHO) also includes a standard on patient confidentiality, questionnaires could be developed to serve as privacy protection and education tools for each clinic or hospital unit for performance improvement initiatives to facilitate legal compliance as well as quality improvement.

The majority of patients in this study valued their privacy and had high or "pretty good" levels of trust in their health care organization to protect that privacy. In an era of eroding public trust, this finding brings good news and merits proactive strategic planning to maintain that patient trust. Understanding how the specialty clinics in which this study was conducted have maintained patient trust provides an opportunity for the health care organization to review and replicate what is working in these specialty clinics. As health care organizations provide improved education that raises patient awareness of both primary and secondary uses of their personal health information, there is an increased risk that trust will be eroded rather than maintained.

Placing privacy and confidentiality statements on a web site is a first step, but also educating patients about privacy risks and responsibilities will help them make informed decisions and will, presumably, build continued trust in their health care provider and the health care system. First educating the providers about health care data and information flow will provide a foundation for them to provider personalized education for their patients. While we need to educate patients about potential benefits of using their data for medical research, we also need to educate patients about the benefits of sharing de-identified data to improve health care outcomes

for the nation. Which models of patient education are most effective with regard to privacy protections for their personal health information have not yet been studied.

Research Implications

High-profile studies have made media headlines in the past few years, and served to erode public trust in medical research. A poll (Gallup, 2000) of 1000 consumers found 70% did not think medical researchers should have access to confidential medical records. In reality, most health care organizations and IRBs permit use of confidential medical records for research, and without patient permission, but within parameters of protecting identifiable data and promoting research that increases our understanding of health, illness, and patient outcomes. Patients understand that a certain portion of their medical information must be available for administration of proper care, and yet only 52-60% of subjects studied thought their data would go to an insurance company or billing department. In our study, 91 participants, (or 98.89%) thought that their medical information would *not* go to a research study or a marketing department. In actuality, however, secondary uses of medical information, without patient consent or awareness, are quite common. According to the Wisconsin Data Privacy Project (ACLU, 2001) there are few prohibitions against secondary uses of health information, and identifiable or encoded data are all too often shared or released with little regard for data integrity or patient authorization.

Patients are familiar with consent forms for clinical trials and surgical procedures because written authorization is a requirement. They are not as familiar with the many databases to which researchers and marketers may have access, without patients being routinely offered appropriate consent or objections to disclosure (ACLU, 2001). The databases include those that maintain information on birth and death records, communicable diseases, and cancer

rates. Consent forms may need to be changed to include permission to use aggregated and anonymous data. And additional studies that explore patients' perceptions of trust, risk, and privacy of their personal health data are needed.

Summary and Conclusions

In general, the trust model described by Etzioni (2001) seems to describe subjects in this pilot study. Patients are still operating under a trust model that considers their providers trustworthy and that their information will only be utilized for their benefit. Patients (n=92) seemed confused about what happened to their data after they provided it for an outpatient clinic visit, and they were generally unaware of secondary uses of the personal health information. Within this context, nearly 85% of patients studied reported "total" to "pretty good" levels of trust in Duke University's health care system, and less than 5% indicated they didn't care much about privacy of personal health information in their medical records.

This pilot study suggests a need for educational programs to increase patients' level of awareness and understanding of where and how their personal health information is stored and shared. Additionally, patients might benefit from education about technology solutions that help protect their privacy; audit trails, encryption, biometric authorization, and techniques to de-identify data for research may actually make computerized patient records *more* secure than paper. While near-term efforts to increase patient education and awareness may increase problems of mistrust, the long-term effects of providing accurate and honest information for patients with respect for privacy in their medical records merit further study.

References

American Civil Liberties Union (ACLU). (2001). *Wisconsin Data Privacy Project.* Retrieved October 14, 2002, from http://www.aclu-wi.org/issues/data-privacy/.

Anonymous. (2001). Compliance delays proposed, opposed. *Health Management Technology*, 22(11), 8.

Association of American Medical Colleges. (2001). Guideline for academic medical centers on security and privacy: Practical strategies for addressing the Health Insurance Portability and Accessibility Act. Retrieved October 14, 2002, from http://www.aamc.org/members/gir/gasp/.

Callas, E., & Brockmeier, K. (2001). HIPAA compliance readiness assessment: A case study. *Healthcare Financial Management*, 55(10), 40-44.

Centers for Medicare and Medicaid Services (CMS). (2002). *Health Insurance Portability and Accountability Act of 1996 (HIPAA).* Retrieved October 14, 2002, from http://www.cms.hhs.gov/hipaa/default.asp .

Craig, M. (2001). HIPAA as a process reengineering challenge: applying portfolio analysis techniques to optimize compliance strategy. *Journal of Health Care Finance*, 28(1), 1-6.

Duke University Health System (DUHS). (n..d.). *Patient Confidentiality Statement.* Retrieved October 14, 2002, from http://dukehealth.org/patients_visitors/confidentiality.asp .

Etzioni, A. (2001) Balancing medical innovation and patient confidentiality. *The Pfizer Journal*. Giorgianni, S. (ed.) 5(3): 1-37.

Gallup Organization. September, 2000. *Public attitudes toward medical privacy.* Princeton, NJ: Gallup Organization.

Goold,S.D. and Klipp, G. (2002) Managed care members talk about trust. *Social Science & Medicine*. 54(6): 879-888.

Hammond, W. Ed (2001). How the Past Teaches the Future: ACMI Distinguished Lecture. *Journal of the American Medical Informatics Association*, 8, 222-234.

Hippocratic Oath. (2000). Retrieved October 14, 2002, from http://classics.mit.edu/Hippocrates/hippooath.html .

Kibbe, D. & Bard, M. (1997). How safe are computerized patient records. *Family Practice Management.* Retrieved October 14, 2002, from http://www.aafp.org/fpm/970500fm/lead.html .

Kirby, D. (2002). *HIPAA concepts, background, & impact*. Retrieved October 14, 2002, from http://staff.dukehealth.org/HIPAA/HIPAA_Concepts_Background_082502.pdf .

Lester, T. (March 2001). *The Reinvention of Privacy*. Atlantic Monthly: 27-39.

Liu, S. & Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional*, 3 (1) 27-32. Retrieved October 14, 2002, from http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm .

Medical Information Bureau (MIB). (2002). *About us*. Retrieved October 14, 2002, from http://www.mib.com/html/about_us.html .

Moynihan, J (2001). Realizing HIPAA benefits requires organizational change. *Healthcare Financial Management*, 55(10), 98-99.

National Institute of Standards and Technology. (2002).*Guidelines on firewalls and firewall policy.* Retrieved October 14, 2002, from http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf.

National Institute of Standards and Technology. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems.* Retrieved October 14, 2002, from http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.

National Research Council. (2000). *Improving access to and confidentiality of research data: report of a workshop Committee on National Statistics.* Mackie C. and ,Bradburn N. eds. Washington, DC. National Academy Press.

National Research Council. (1997). *For the record: protecting electronic health information Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure*. Retrieved October 14, 2002, from http://www.nap.edu/catalog/5595.html .

Office of Technology Assessment. (1993). *Protecting privacy in computerized medical information OTA-TCT-576*. Retrieved October 14, 2002, from http://www.wws.princeton.edu/~ota/ns20/year_f.html

Pritts J., Goldman J., Hudson Z., Berenson A., & Hadley E. (1999, August). The state of health privacy: an uneven terrain, *Health Privacy Project*. Retrieved on October 14, 2002, from http://www.georgetown.edu/research/ihcrp/privacy/statereport.pdf .

Rothenberg,K.H. and S.F. Terry (2002). Human genetics. Before it's too late--addressing fear of genetic information. *Science*. 297(5579):196-7

Shalala, DE. (1998). *July 31, 1997 Protecting privacy of health information, Address to the National Press Club.* Retrieved on October 14, 2002, from http://town.hall.org/radio/Club/071494_club_ITH.html .

The Pfizer Journal. (2001) *Balancing medical innovation and patient confidentiality.* Giorgianni, S. (ed.) 5(3): 1-37.

U.S. Department of Health and Human Services (HHS). (2002). *HHS issues first major protections for patient privacy: Consumers gain new controls over records beginning April 2003.* Retrieved October 14, 2002, from http://www.hhs.gov/news/press/2002pres/20020809a.html .

Voran, D. 1998. Privacy, security, and shared access - can confidentiality be protected in a networked society. *Bioethics Forum*, 14(3/4): 43-48. Retrieved on October 14, 2002 from http://www.midbio.org/mbc-forum14-3.htm .