Wallis, K. & Rice, R. E. (2006).
Technology and health information privacy:
Consumers and the adoption of digital
medical records technology.
In M. Murero & R.E. Rice (Eds).
The Internet and health care: Theory, research and practice
(pp. 279-311). Mahwah, NJ: Lawrence Erlbaum Associates.

Chapter 14

Technology and Health Information Privacy: Consumers and the Adoption of Digital Medical Records Technology

Kier Wallis
University of California, Santa Barbara

Ronald E. Rice
University of California, Santa Barbara

NATIONAL AND REGIONAL IMPLEMENTATIONS OF DIGITAL MEDIAL RECORDS

This chapter investigates consumer concerns, knowledge, and level of awareness of digital medical records (DMRs) technology, and privacy and identifies those factors most strongly related to consumers' potential adoption or rejection of the technology.

Digital Medical Records

The nature of health care in the United States, largely HMO-based, is driving the implementation of DMRs, also known as electronic health records (EHRs) in response to a demand for data transparency. Gunter and Terry (2005) described the EHR as "a longitudinal collection of elec-

---

*The authors would like to acknowledge, and thank, the six regional health care administrators who shared their thoughts during the stakeholder interviews; the students and employees who participated in the focus groups and surveys; the Arthur N. Rupe endowed Professorship in the Social Effects of Mass Communication, and an Undergraduate Research and Creative Activities grant, for financial support; and especially Mr. Mike Skinner, Executive Director of the SBCCDE, for his guidance, contacts, expertise, and support. Due to space limitations, much detail is missing in this chapter; see http://www.comm.ucsb.edu/faculty/rrice/sbccde.pdf for complete literature review and tables.

tronic health information from individual patients and populations" (p. 2). Concerns about medical mistakes, the widespread occurrence of ambulatory care, and the increasing responsibility among patients for their health care are among the reasons DMRs have become a priority for health care providers. However, providers must also respond to patient demands for privacy, access, correction, and consent, as well as legislative demands for legal compliance (Gunter & Terry, 2005).

DMRs are credited with improving health care by reducing medical errors, eliminating handwritten clinical notes, enabling error-reducing technologies, increasing the consistency of medical records, and providing data for research (Reynolds, 2003). Several studies have also cited benefits for both physicians and patients (Hassol, Walker, Kidder, Rokita, Young, et al., 2004; Joustra-Enquist & Eklund, 2004). For example, Wang, Lau, Matsen, and Kim (2004) developed a web-based personal health record (PHR) for patients to collect and manage their health information (medical history, past surgeries, medications, and allergies), to request self-referrals, and to store a record of their consultations. Thirty-two patients completed a survey in which 85% of respondents were satisfied with the usability and 94% were satisfied with the overall online referral process. Using DMRs in hospital databases was demonstrated to help ensure consistent and correct coding by physicians, as well as context-sensitive treatment (Muller, Burkle, Irps, Roeder, & Prokosch, 2003). A study of the 30% of physicians using DMRs in 2003 reported that 78% saw an improvement in patient satisfaction, 87% said it allowed them to deliver better care, and 89% saw improved compliance with managed care (Harris Interactive, 2003). One health record exchange pilot project involving three Indianapolis hospitals found an average reduction of $27 in costs per patient visit (mostly from reducing waste and duplication; Ferris, 2005b).

Connecting for Health (2005) reported on a series of focus groups and national surveys investigating the public's awareness of and willingness to adopt an EMR. They found that people have a limited understanding of health IT today. When presented with messages about the potential benefits of PHRs, more than half said they had never thought about concepts such as (a) "I should have access to my health information anywhere, anytime," or (b) "My own online medical record would help me get all my doctors on the same page when they treat me." Yet, 72% of the respondents to their 2004 survey strongly or somewhat agreed that they wanted to be involved in medical decisions that affect them, and having their own medical record would help them make better decisions; and 62% strongly or somewhat agreed that they would like to have all their health information in one place, and obtain it with a click of the mouse.

Participants in the 2003 focus groups reported a strong desire to have total control of their personal health information, wanting the power to decide who could and could not access their record and an expectation that they should provide explicit consent to any access. However, preferences for how to access this information varied by age; under 45, the Internet was the most preferred channel (33%), whereas over 45, paper was most preferred (34%). Their 2003 survey of online Americans (Connecting for Health, 2003) found these medical services desired by the respective percents: e-mail my doctor (75%), track immunizations (69%), note mistakes in record (69%), transfer information to new doctors (65%), and get and track test results (63%). Still, 96% were most comfortable with their primary care doctors having access to their medical record (58% preferred their doctor's office to be the host of an online medical record system), and less comfortable with the idea of having family members (69%) and their health insurance company (65%) having access.

The development of the current DMR model in the United States has focused on establishing data interoperability and comparability (Gunter & Terry, 2005), using a system in which patients "pull" or censor certain information in their records, although the exact amount of patient authority remains unclear. Such a pull system is intended to maximize the flow of patient data, enabling valuable research, although some critics worry it may result in a loss of patient privacy and confidentiality.

Regional health information organizations (RHIOs) are responding to this initiative. More than 100 have been formed, comprising community institutions such as hospitals, physicians, government agencies, insurers, laboratories, employers, and consumers. And more than 20 are already exchanging health care information (Ferris, 2005a). But funding and cost recovery for RHIOs is still very uncertain. There is no agreement yet as to whether individuals, insurance companies, government agencies, hospitals, or others who pay medical bills will fund these systems (Ferris, 2005b).

THEORY: DIFFUSION OF INNOVATIONS, TECHNOLOGY AND HEALTH INFORMATION PRIVACY

Rogers's (1983) Diffusion of Innovations theory, and Smith, Milberg, and Burke's (1996) Information Privacy theory will be used to frame the investigation of the relationship between technology and privacy, and their relationship to the implementation of DMRs in Santa Barbara County.

Technology Diffusion

A new technology faces various challenges to successful diffusion within its potential community (Aydin & Rice, 1991; Davis, 1993; Rogers, 1983). Different obstacles apply at every level, influencing adoption and reinvention of an innovation (Johnson & Rice, 1987; Rice & Anderson, 1994), and among prospective consumers (Davis, 1993; Demiris & Eysenbach, 2002; Mandl, Szolovits, & Kohane, 2001; Rogers, 1983). Of particular interest to this study are the characteristics of the diffusion process among the upcoming generation of consumers, as they have greater familiarity and comfort with technology.

Rogers (1983) identified five characteristics of innovations central to the effective diffusion of any new technology: relative advantage, compatibility, complexity, trialability, and observability. Consumers perceiving a new technology to rate high on these characteristics, with the exception of complexity, are more likely to adopt the technology. Other models emphasize the importance of characteristics similar to those established by Rogers. For example, the technology acceptance model (Davis, 1993) recognizes the importance of consumers' attitudes toward a technology as a main determinant of their actual technology use. Davis (1993) identified two main technology components influencing consumers' attitudes—perceived usefulness and perceived ease of use—which correspond with Rogers's (1983) descriptions of relative advantage and complexity, respectively. Also, Mandl et al. (2001) noted six desirable characteristics of DMRs: comprehensiveness, accessibility, interoperability, confidentiality, accountability, and flexibility, all of which reflect the five innovation characteristics.

Relative advantage is the "degree to which an innovation is perceived as better than the idea it supersedes" (Rogers, 1983, p. 15). In the case of individuals' DMRs, relative advantage may be conceptualized as the innovation's benefits in comparison to traditional paper records, such as the improvement of patient care and safety, the reduction of medical errors, and the positive financial return to health care organizations (Chin, 2001; Wang, Middleton, Prosser, Bardon, Spurr, et al., 2003). Some of the qualities that might indicate relative advantage for consumers include accessibility, accountability, and flexibility (Mandl et al., 2001). *Compatibility* is "the degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters" (p. 15). Innovations inconsistent with the value system of potential adopters are likely to be rejected. Important consumer values may include personal health and health of loved ones, the ability to control their own health care, and privacy (Alpert, 2003; Jeffords, 1999; Mandl et al., 2001). *Complexity* is "the degree to which an innovation is perceived as difficult to understand and use" (p. 15). Not all consumers are equally able to use, understand, and benefit from new technologies. An important consideration under complexity is self efficacy, or one's perceived ability to perform a specific task (Bandura, 1997). Thus, individuals who have greater expertise with Internet technology and use it more frequently are more likely to be comfortable adopting a new Internet-based technology. However, some health care recipients, such as the elderly or individuals with chronic illnesses, may not be as adept at using the Internet, or have functional limitations preventing them from access (Demiris & Eysenbach, 2002). *Trialability* is "the degree to which an innovation may be experimented with on a limited basis" (p. 16). This may pertain to the extent of the commitment required of the consumer, or to the user's ability to release and then later restrict access to a DMR (Mandl et al., 2001). *Observability* is "the degree to which the results of an innovation are visible to others" (p. 15). In diffusing a new technology, publicly displaying an innovation's positive consequences is likely to aid in reducing consumer uncertainty surrounding the new technology. Although uncertainty is an inevitable companion to innovation (Rogers, 1983), consumers' outcome expectations have been found to impact actual technology use (Compeau & Higgins, 1991).

Privacy and Technology

Public opinion has demonstrated the growing importance of privacy in today's information-saturated society (Udo, 2001). Metzger and Docter (2003) reviewed public opinion polls, industry positions, enacted legislation and proposed legislation about online privacy protection, between 1998 and 2001. They considered online privacy concerns to include anonymity, intrusion (spam, data mining), surveillance (individual and public—especially since the Uniting and Strengthening America Act 2001, commonly referred to as the Patriot Act), and autonomy. Over two thirds of one survey's respondents felt that their ability to control the collection of personal information was extremely important (Harris Interactive, 2003). Most (85% to 97%) Web sites collect at least one type of personal information, generally without user consent, whereas other sites also sell customer information to third parties. Averaged across a number of polls, three quarters of respondents (74%) were "very" or "somewhat" concerned about privacy when using Internet, though concerns declined a bit with increased Internet experience, and when using familiar e-commerce sites. Six primary concerns about users' rights emerged from this review with from 60% to 89% supporting or concerned about: Notice, choice, access, security of information, enforcement, and children's online privacy rights. Metzger and Docter (2003) concluded that "existing and proposed Internet privacy legislation fails to address the full range of consumers' concern" (p. 366), with little fulfillment of the six principles. Most sites rely on self-regulation, and there is little prospect of new legislation protecting individuals' privacy being passed, especially after the increased powers of law enforcement agencies after the terrorist attacks of 9/11 in the United States.

The risks and benefits associated with information technology have resulted in tension between the information-collecting organization and the consumer, and the consumer is caught in the position of both victim and beneficiary. As competitors in the marketplace have harnessed information technology to collect and assemble data into usable and marketable forms, the general public is not convinced that the benefits of information technology outweigh its costs (Culnan & Armstrong, 1999). Having lost the ability to control collection and use of personal information raises concerns in accordance with Westin's (1967) definition of privacy as the ability to control the collection and use of personal information. Smith et al. (1996) identified four factors that affect an individual's level of privacy concern: (1) unauthorized secondary use, (2) improper access, (3) collection, and (4) errors.

The traditional realm of information privacy has been affected by the rapid growth of computer and digital technology, leading to an increasing number of medical records stored in a digital or electronic format (Jeffords, 1999; Li & Shaw, 2004; Nasser & Alpert, 1999; Swartz, 2004). The transfer of data from traditional paper to the new digital format has resulted in increased concerns among the patient population, and has prompted at least some new legislation to establish privacy guidelines (Alpert, 2003; Fedorowicz & Ray, 2004; Li & Shaw, 2004; Swartz, 2004). In the Connected for Health (2003) survey of online users, nearly all (91%) were very concerned about privacy and health information security, but most felt that technology provides appropriate protections. People with chronic illness and frequent health care users were less concerned about privacy and security.

The most notable legislation relevant to DMRs is the Health Insurance Portability and Accountability Act (HIPAA), which is designed to ensure the integrity of patient information as it travels between health care providers, insurers, and data-clearing houses (Epstein, 2002; Fedorowicz & Ray, 2004; Health Privacy Project, 2004; U.S. Department of Health and Human Services, 2000; 2001). HIPAA establishes requirements for health care organizations intended to maintain an acceptable level of privacy, to be enforced by severe punishments for the misuse of patient information. Health care entities, specifically health plans, health care clearinghouses, and health care providers who conduct transactions electronically, were required to achieve HIPAA compliance by April 14, 2003 (U.S. Department of Health and Human Services, 2004). Recent public comments (more than 500 responders and more than 5,000 pages) on the National Health Information Network (NHIN) and health records exchanges in the United States, provided to the Department of Health and Human Services, emphasized that such a system must be patient-oriented, with safeguards to protect personal health information privacy (Brewin, 2005).

A recent integrated set of recommendations (Connecting for Health, 2005) argued that such a health information environment must: (a) facilitate effective connectivity for the delivery of high quality health care; (b) provide timely access to information; (c) empower patients to access and control their own information and contribute to the quality of care provided; (d) support the application of "intelligent" tools to improve health and health care; (e) facilitate the appropriate aggregation of data for public health, research, and quality assessment; and (f) enable improvements in the quality of clinical care. Patients must be able to: (a) choose whether or not to participate in sharing personally identifiable information; (b) exercise their rights under HIPAA; (c) control who has access to their records (whether in whole or in part); (d) see who has accessed their information; (e) review, contribute to, and amend their records (without unreasonable fees); (f) receive paper or electronic copies of their information; and (g) reliably and securely share all or portions of their records among institutions. Once patient consent has been granted for a certain type of information access, however, information should be able to be accessed freely in a trusted environment.

Relationship Between Technology Adoption and Health Information Privacy

The factors contributing to privacy concern may be discussed as subsets of many of the technology diffusion characteristics, especially relative advantage, compatibility, and complexity. Privacy concerns corresponding to the proposed security of DMRs are an important factor when evaluating the technology in terms of relative advantage. Several improvements over paper records have been cited, including increased security (Shoesmith, 2001), and improved health care quality (Alpert, 2003; Shoesmith, 2001). Critics of DMRs are concerned that the misuse of information (Alpert, 2003) might ultimately result in a compromised level of patient care, negating any advantage of the digital system in comparison to paper records. The CHCF found that one in six adults reported having done something "out of the ordinary" to prevent the disclosure of their medical information, including avoiding medical care all together (California HealthCare Foundation, 1999). Therefore, improper access, unauthorized use, and error, whether system or human error (Smith et al., 1996), may contribute to a lower evaluation of DMRs in terms of relative advantage.

Similar concerns reverberate in terms of the technology's compatibility with consumers' current value systems and needs. Privacy is an important value to consumers (Alpert, 2003; Jeffords, 1999; Mandl et al., 2001), and it is likely that any privacy violation would reduce consumers' beliefs that DMRs are compatible with their value systems. Also, the collection of information for DMRs, depending on the level of communication between the collecting organization and individual, might be linked to compatibility, as consumers have been found to value control over their personal information and its disclosure to third parties (Milberg, Smith, & Burke, 2000). Errors would indicate that the digital system is overly complex for its intended users, and due to the sensitive nature of personal medical information, the possibility for error is extremely important in determining a consumer's adoption or rejection of DMRs. If an individual is not convinced that the system will store or provide reliable and accurate data, it is unlikely that he or she will spend time with the system, leading to rejection.

METHODS: SITE, STAKEHOLDER INTERVIEWS AND FOCUS GROUPS

The study used a variety of methods to summarize, integrate, and identify factors influencing potential users' responses toward DMRs. First we discuss the site, the stakeholder interviews and focus group discussions, and their results.

Site: SBCCDE

The Santa Barbara County Care Data Exchange (SBCCDE), a major regional health infrastructure project, is in the process of implementing digital medical records (DMRs) technology in Santa Barbara County, California, and is subject to evaluation by the general public and medical community (Care Science, 2005). The SBCCDE cites its mission as "assisting all physicians, caregivers, and consumers in Santa Barbara County to locate and facilitate the sharing of patient data held by multiple health care organizations . . . thereby increasing the quality, safety, and efficiency of care delivery." The SBCCDE, founded in 1998, is currently testing its technology, the Care Data Exchange (CDE), and preparing for its diffusion into local hospitals, health care organizations, and the community at large (McGee, 2003). The SBCCDE project is a small-scale extension of the larger national plan to institute a national electronic health information infrastructure (McGee, 2003; U.S. Dept. of Health and Human Services, 2004). (For an online demonstration/explanation of Healthcare Collaborative Networks, prepared in 2003, using three case studies—preventative care, outbreak alert, and monitoring adverse drug events—see: http://www.connectingforhealth.org/resources/HCN_24.html.)

Stakeholder Interviews

Six interviews were conducted with individuals representing institutions the executive director of the SBCCDE identified as major stakeholders in the CDE project, including Cottage Hospital, Santa Barbara Regional Health Authority, Sansum Medical Foundation, Santa Barbara Public Health Authority, a community business professional, and a participating physician. The interviews, all conducted by the same researcher, lasted approximately 90 minutes, and were tape-recorded to facilitate later analysis. The interviewees answered 12 questions on behalf of their organization, primarily focusing on the organizations' roles within the CDE and their perceptions of the technology in terms of privacy, security, and operability. The stakeholders were also asked to evaluate the CDE's advantages and disadvantages, and estimate the level of consumer participation their organization expected following the system's implementation.

Focus Groups

A focus group is a qualitative data-gathering approach that offers insight into target populations and new concepts, provides a basis for developing questionnaire or survey content, and allows the exploration of categories that would be restricted by quantitative methods (Fuller, Edwards, Vorakitphokatorn, & Sermsri, 1993; Knodel, 1993; Krueger, 1993; Morgan, 1993; O'Brien, 1993; Wolff, Knodel, & Sittirari, 1993). Focus groups are a common method of testing new technologies (Williams, Rice, & Rogers, 1988).

From the stakeholder interviews and the prior literature review, we developed questions for focus group discussions. A pilot focus group was conducted with undergraduate students to identify any problems with the discussion guidelines. The five remaining focus groups consisted of three undergraduate groups, one graduate student group, and one employee group. Of the three undergraduate groups, one group was students who had identified themselves as having a chronic illness, such as diabetes or asthma. This distinction was made based on literature demonstrating that patients' experiences with health technology may differ among healthy and unhealthy patients (Ralston, Revere, Robins, &

Goldberg, 2004; Ziebland, Chapple, Dumelow, Evans, Prinjha, & Rozmovits, 2004).

Each focus group had two main concepts for discussion. The first was a conceptual understanding of DMRs. The moderator read an excerpt from an article in PC Magazine (September 26, 2001) describing the concept and then opened discussion of DMRs by asking questions about the participants' views and concerns regarding the new technology. The second concept was the local implementation of the technology, with the moderator reading a paragraph written by the researchers to introduce the details of the system and concepts.

RESULTS FROM STAKEHOLDER INTERVIEWS AND FOCUS GROUPS

Stakeholder Interviews

The interviews are the statements and opinions of individuals on behalf of the organization or population they represent. Following completion of the interviews, researchers designated the 6 stakeholders as nonprofit or profit organizations with SBPHD, SBRHA, and the community-at-large as nonprofit stakeholders, and Cottage Hospital, SFMC, and clinicians as profit stakeholders. Table 14.1 summarizes these answers, providing those responses that were common to both kinds of organizations, and those unique to each of the two types of organizations.

Focus Groups

Table 14.2 provides the focus groups questions asked, and summarizes the participants' responses to two of these, according to group type. The focus groups' responses were also analyzed according to word frequency. First, all responses within each of the 15 questions were combined across the six focus groups. Then, the 15 questions were grouped into three categories: (a) personal or individual concern (Questions 1, 2, 11 and 12); (b) others' concern (Questions 3, 8, 13, 14, and 15); and (c) advantages and disadvantages of DMRs (Questions 4, 5, 6, 7, 9, 10, 11). "Stop words" ("a," "and," "the," "etc.") were removed, and words were "stemmed" (all variants were converted to one form, such as "patients" and "patient," or "you're" and "you"). Then a computer program went through the text in the three categories, identified and counted each unique word, and sorted the words alphabetically according to decreasing frequency. Table 14.3 lists the words occurring five or more times

TABLE 14.1
Summary of Responses to 12 Questions of Stakeholder Interviews

Question	*Common Among Profit and Nonprofit Stakeholders*	*Unique to Nonprofit Stakeholders*	*Unique to Profit Stakeholders*
1. Years current org		7.1 years	9.3 years
2. Years medical field		23.9 years	32.7 years
3. Role in CDE Possible gains or losses?	Active in CDE's development. Member on CDE board. Contribution of data, resources.	One organization serves as insurance company to the CDE. Community is unaware of CDE. Security violation would equal loss.	Recognize the benefit to community. Unclear direct benefits to organizations. Previous concern over competitive advantage. Initial implementation requires money and time.
4. CDE's purpose/function within SB community	Improved quality of care. Improved overall health outcomes. Coordination of care, medical programs.	Reduction of test and prescription duplication.	Clinicians will have a single access point to services outside of local network.
5. Involvement with CDE's development	Active participation on CDE board throughout CDE's conception and implementation.	Unaware of general community involvement in CDE (prior to establishment as nonprofit in 03/2004).	Contribution of staff, resources, funding, data.
6a. Advantages of instituting CDE	Improved quality of care. Save time by consolidating medical information into individual digital records.	Reduced labor costs with capabilities of electronic system.	Records available quickly and in a usable format.
6b. Disadvantages of instituting CDE	"Challenges" or "Things to think about." Development and maintenance costs. Issues remain to be resolved.	CDE is not a substitute for personal interaction. Patients' reactions remain unknown. Anxiety over security and privacy issues.	CDE participants have separate and different technology systems. Getting started. Technology is a hurdle; "CDE is not proven state-of-the-art technology."

(*Continued*)

TABLE 14.1
(Continued)

Question	*Common Among Profit and Nonprofit Stakeholders*	*Unique to Nonprofit Stakeholders*	*Unique to Profit Stakeholders*
7. Concerns about CDE's current testing	Adequacy and accuracy of CDE's data.	Good planning and communication between CDE management and testing clinicians is vital. Consumer doesn't have concerns because "out of the loop."	Source of future funding is unclear. Physician must see value in the CDE. CDE needs to have all glitches resolved. CDE must accurately identify individual patients.
8a. Definition of operability	How the system works. System's ability to retrieve correct data.		Accessibility and navigability of CDE to user with standard technology.
8b. Definition of security	Technical protection of data via user authorization.	Can system be hacked into?	Access must have clear guidelines and procedures.
8c. Definition of privacy	Patients to be aware that their medical data is shared with CDE and aware of who has access.	Protection and confidentiality of medical records.	HIPAA compliance.
9a. Operability rating	Seems to be working, but CDE is still in testing phase.	Unsure if data is rich enough.	
9b. Security rating	In theory, CDE is secure, but technology has yet to be implemented.	Outside evaluation passed CDE.	Important to achieve security.
9c. Privacy rating	In theory, CDE seems to be private, but technology has yet to be implemented.	Outside evaluation passed CDE. CDE continuously working on privacy issues.	Important to achieve privacy.
10a. Characteristics advantageous to community acceptance	National attention for Santa Barbara. Improved and safer treatment of patients.	Patients can avoid redundant testing and blood work, saving time and money. Paper medical records eliminated.	Less effort for patient to coordinate different physicians and specialists. CDE consumer portal.
10b. Characteristics disadvantageous to community acceptance	Not all patients have adequate technology, Internet access, or the skills to use the CDE. Security and privacy concerns over data on Internet.	CDE development has lacked community involvement and input.	Security and privacy concerns about insurance companies and employers access to medical records.
11. Consumers' rights to regulate and access medical records	Law dictates consumers' rights. By law, patients have right to access their medical records.	Patients have right to request record be removed from system.	HIPAA provides for those people managing patient's care to have access to medical records. Question of consumers' abilities to interpret data in medical record.
12. Consumer participation in CDE	Consumer portal is on hold. Some organizations are skeptical of consumer use. Patients to use CDE to view test results, get up-to-date medical information. Consumer use will vary according to characteristics of patient population. People are becoming increasingly active in health care.	Low-income and uninsured patients won't be likely to access the CDE. People will review the log of users accessing their medical record.	Chronically ill patients are more likely to use CDE; may participate in disease state management. People to view test and lab results, request appointments and medicine.

TABLE 14.2
Focus Group Topics, and Summary Themes From Two of Them, by Type of Focus Group

Focus Group Topics

Part I: Concept of Individual Digital Medical Records

A. Privacy
  1. What information do you think your medical record contains? How would you use such information if you had access to it?
  2. What rights do you think you have regarding your medical record?
  3. What information from your medical record can doctors share with other health care providers or health institutions?
  4. What concerns or questions do you have regarding the availability of your medical records?

B. Read a short description of individual digital medical records on the conceptual level.
  5. How do you think digital medical records would compare to current paper-based health care records?
  6. What risks or disadvantages come with the implementation of this technology?
  7. What benefits or advantages come with the implementation of this technology?
  8. How would you feel about having your physician or health care provider implementing such digital records?

Part II: Local Implementation of Digital Medical Records

C. Read a short description of the local implementations of CDE technology in Santa Barbara.
  9. In the context of digital medical records' implementation in Santa Barbara County, what risks or disadvantages do the residents of Santa Barbara face following the implementation of this technology?
  10. In the context of digital medical records' implementation in Santa Barbara County, what benefits or advantages will the residents of Santa Barbara encounter following the implementation of this technology?
  11. Would you access your own medical record if given the opportunity? If so, for what purpose? If not, why? (Remember what they said medical records contained . . . Q1).
  12. What do you think about other consumers accessing their medical records? For what purposes might they access their medical records?
  13. What do you think about being able to see a list of individuals and institutions that have authorized access to your medical record?
  14. What do you think about being able to see a log of individuals who have had authorized access to your medical record?
  15. Would you be willing to sign a waiver allowing physicians and other authorized parties to view your medical record?

Q4. Concerns or Questions	*Healthy Students*	*Chronic Illness*	*Graduate Students*	*Employees*
Are records transferred when a patient changes doctors?			X	
Are you allowed to have access to your records?	X			
Can a child look at her parents' record?	X			
Can parents' view their child's record?		X		
Can responsibility for an individual's record be transferred to a third party if the individual is capable of caring for herself?	X			
Is medical information understandable to avg. person?	X			
Marketing				X
None		X		
Parties should only be able to access the information they need			X	
Patient should be able to put medical information in context	X			
Too young to have thought about it	X			
What information is available to insurance companies?			X	X
Who do you have to talk to get old records?	X			
Who has access?			X	

(Continued)

TABLE 14.2
(Continued)

Q7. Benefits and Advantages of Digital Medical Records	*Healthy Students*	*Chronic Illness*	*Graduate Students*	*Employees*
Ability to view access log	X			
Accurate diagnoses	X	X		
Benefits patients with illnesses		X		
Brings integrity to medical field		X		
Convenience for doctors	X		X	
Easier to change doctors	X			
Easier to keep track of medication		X		X
Eliminates repeat paper work	X		X	
Ideal for emergency	X			
Ideal for travel	X	X		X
Information used for research		X		
No risk of losing files (in a fire, etc.)	X			
Patient access			X	
Quickly accessible	X			
Reliability	X			
Well organized	X			

TABLE 14.3
Focus Groups' Words Mentioned Five or More Times in Responses to Three Categories of Questions

Personal

I (77, 9.5%), doctor (37, 4.6%), yes 33 (4.1%), people (20, 2.5%), access, check, history (19, 2.3%), don't, might, record, want (17, 2.1%), curious, know (13, 1.6%), information (12, 1.5%), medication (11, 1.4%), need, right (10, 1.2%), family, insurance, look, stuff (9, 1.1%), blood, disease, go, medical (8, 1%), illness, parents, privacy, thing (7, .9%), allergies, ask, good, keep, maybe, visit (6, .7%), company, file, health, patients, think, type, vaccinations, whether, wouldn't (5, .6%)

Others

I (106, 13.4%), yes (62, 7.9%), don't (39, 4.9%), access (29, 3.7%), doctor (25, 3.2%), want (23, 2.9%), people (17, 2.2%), know (16, 2%), long (15, 1.9%), care, information (13, 1.6%), look, record (12, 1.5%), think (11, 1.4%), might, wouldn't (9, 1.1%), good, health, need, thing (7, .9%), fine, interested, list, problem, share (6, .8%), asked, authorization, change, company, consent, definitely, insurance, maybe, permission, right (5, .6%)

Advantages and Disadvantages

record (47, 4.9%), I, easy (42, 4.3%), access (41, 4.2%), people (40, 4.1%), doctor (38, 3.9%), don't (33, 3.4%), paper (27, 2.8%), information (21, 2.2%), computer (20, 2.1%), patient (17, 1.8%), thing (15, 1.6%), go (14, 1.4%), look (12, 1.2%), cost, hacker, health (10, 1%), change, file, know, might, think, wouldn't (9, 9%), ask, Santa Barbara, digital, having (8, .8%), better, good, help, history, lose, medical, problem, transfer (7, .7%), different, emergency, seems, system (6, .6%), advantage, allow, benefit, copy, diagnosis, hard, hospital, long, lot, older, online, outside, privacy, saves, time, want, wrong (5, .5%)

Note. Values are the number of times mentioned, and percentage of the specific word's occurrence within the top 160 words.

within each group of questions. (The words used for both the thematic and word frequency analysis were the text provided by an independent note-taker, and it is possible that some bias may be present among the words. For example, the one person who took all the notes may have summarized participants' comments in ways that systematically emphasized some words and meanings over others.)

Expectations About Use

The prospect of DMRs technology was exciting to the stakeholders and focus groups, with both groups recognizing the technology's advantages in comparison to current paper records and the possible health care improvements. Stakeholders were not in complete agreement as to how consumers would participate in or use the CDE, and the nonprofit stakeholders felt that their lower income and uninsured clientele would not reap the benefits of the CDE's consumer portal. The focus group participants, when asked if they would access their DMRs, were also not in agreement. The majority of participants said that they would, for reasons ranging from curiosity to self-treatment, but the graduate and employee groups exhibited greater hesitancy due to concerns involving health insurance and employment. It is possible that to successfully diffuse the CDE, participants' age and financial independence should be considered when developing appropriate marketing campaigns.

Meanings of "Privacy"

The stakeholders agreed on a general definition of privacy, including patient awareness as a requirement in fulfilling their organizations' obligations to privacy. More generally, stakeholders tended to combine privacy and security, defined as the technological protection of data accomplished through user authorization. Although focus group participants were not asked to define privacy, they identified privacy as a specific concern accompanying the implementation of DMRs, along with the desire to be informed of and exercise discretion over their medical records' authorized users. The general sentiment among stakeholders was that, provided the CDE was in compliance with HIPAA regulations, privacy issues would not be a major problem. In contrast, focus group participants, who were largely unaware of patients' legal rights, overestimated their ability to access and control their traditional medical information, and perhaps as a result were not completely willing to participate in the CDE.

Awareness of Digital Medical Records and CDE

Although the stakeholders discussed the need for patient awareness, the focus group participants confirmed that they had not been properly informed of the technology's implementation and would have appreciated communication between the SBCCDE and the community.

METHODS: SURVEY DEVELOPMENT, MEASUREMENT, AND SAMPLE

Based on central concepts from the literature review, and results from the stakeholder interviews and focus groups, a pilot survey was developed, tested with a small set of respondents, and revised for the formal survey. The final survey contained the following sections and items.

Measures

Individual Characteristics. Survey respondents were asked to rate their *health status* in comparison to other people of the same age and sex on a scale of 1 = very unhealthy to 7 = very healthy. Respondents were also asked to indicate whether or not they had ever had a *chronic illness or health problem*. *Age* was measured by the number of years and months since the respondents' birth. Respondents' *year in college* was measured as 1 = freshman to 4 = senior. Respondents were asked to estimate how much of their *annual expenses* (tuition, housing, food, travel) they earn or pay for themselves (1 = none to 5 = all), and whether or not they pay for their own *health insurance*. A 10-item scale from Jerusalem and Schwarzer (1992) was used to measure *general self-efficacy* (1 = not at all true, 2 = hardly true, 3 = moderately true, 4 = exactly true).

Privacy Attitudes. Eight items measured respondents' *general privacy* attitudes. The items were developed based on frequently cited definitions of privacy, including Warren and Brandeis (1890), "people should have the right to be left alone," and Westin (1967), "people should have the right to control their personal information" (1 = very strongly disagree to 7 = very strongly agree). *Need for privacy* was measured by Buss's (2001) 19-item scale (1 = very strongly disagree to 7 = very strongly agree). Respondents' attitudes toward *organizational privacy* were measured using 11 items from Smith et al.'s (1996) 15-item instrument. The instrument uses four subscales to measure individuals' concerns about collection, errors, unauthorized secondary use, and improper access (1 = very strongly disagree to 7 = very strongly agree). Nine items measured *general concerns about computer privacy*, such as monitoring and hacking (1 = not concerned at all to 7 = very strongly concerned). Twelve items developed from focus group participants' responses to a question about their medical rights, measured respondents' perceptions of patients' medical rights (1 = true, 2 = false), with correct answers identified by the SBCCDE's Executive Director. The number of participants' correct answers was summed.

Technology Use and Expertise. Respondents were asked to indicate the *frequency of their Internet use* from home, work, school (excluding the library), library, or other locations (each 1 = never to 5 = daily). They were also asked to indicate the number of years that they have been using the Internet (including email, web, chat, downloading, etc.). *Web expertise* was measured by 12 questions taken from the Georgia Tech (1998) web survey that asked whether or not the respondent had performed a variety of activities (such as created a web page). The Georgia Tech survey calculated the total number of activities respondents had completed and grouped respondents according to four levels of expertise: 0–3 activities, novice; 4–6, intermediate; 7–9, experienced; and 10–12, expert. *Web fluency* was measured by 17 items taken from the computer-e-mail-web fluency scale developed by Bunz (2004; 1 = very difficult to 7 = very easy). Fluency, according to the Committee on Information Technology (1999), is defined by three concepts: it (1) entails a lifelong learning process, (2) implies personalization of skills on levels of sophistication, and (3) is composed of three kinds of knowledge: contemporary skills, foundational concepts, and intellectual capabilities.

Innovation Attributes. After the individual characteristics and technology use and expertise sections on the questionnaire, survey respondents read two paragraph-long descriptions of DMRs, identical to those used in the focus groups. The scales used to measure the five primary innovation attributes were developed based on the thematic and word frequency results of the focus groups, Rogers's (1983) research, and feedback from the SBCCDE's executive director. Survey respondents were asked to indicate their agreement with items representing the following attributes (1 = very strongly disagree to 7 = very strongly agree). *Relative advantage* was measured using 13 items comparing paper-based and DMRs. *Compatibility* was measured using eight items representing focus group participants' statements of values and needs, with the most prevalent being access, privacy, security, and quality health care. *Complexity* was measured by eight items derived from focus group participants' questions, and statements of concern, disadvantages, and the likelihood of their own individual use and others' use. *Trialability* was measured by three items indicating the extent to which respondents desired the ability to experiment with digital medical records, or reserving the ability withdraw their participation as well. *Observability* was measured using seven items, focusing on support for the innovation's progress and respondents' desire to participate in its development or obtain some physical representation of their participation in the CDE. These items resulted from collaboration between researchers and the SBCCDE's executive director who identified several ways in which the public might observe or experience the results of DMRs.

Technology Evaluation. To measure survey respondents' likelihood of *adoption* of DMRs, the SBCCDE's executive director identified nine consumer actions that would indicate adoption, such as whether a respondent would be willing to sign a consent form releasing their information to the SBCCDE digital database (1 = very strongly disagree to 7 = very strongly disagree). When reviewing the focus group data, researchers noticed a wide variety of statements describing previously unanticipated consumer and administrative uses of DMRs. These statements were compiled along with statements about anticipated uses of the innovation, resulting in 14 items measuring the ways in which participants anticipated they or others might *reinvent* the DMRs (1 = very strongly disagree to 7 = very strongly disagree).

Table 14.4 provides descriptive statistics on the scales and subscales used in the analyses, with scale reliabilities, and, where relevant, subscale principal component values. Descriptive statistics and wording for scale items are available from the Web site listed earlier, though illustrative items from each scale are noted below. Figure 14.1 summarizes the hypothesized relationships between the explanatory overall scales and subscales, and the outcome measures of adoption and reinvention.

RESULTS: DESCRIPTIVE

Individual Characteristics

The sample, composed of undergraduate students taking introductory communication courses at the University of California Santa Barbara, was 76.8% female, 29.8% of respondents were freshmen, 37.8% were sophomores, 26.9% were juniors, and 3.1% were seniors. The SBCCDE Executive Director was particularly interested in the attitudes and knowledge of this population group, as they represent the next generation of medical system users, and have greater familiarity with Internet technology. The majority of respondents described their *health* as at least average, with no more than 8.5% reporting to be below average, and 67.8% as above average; only 17.9% of respondents had ever had a *chronic illness*. A small 7.7% of respondents were personally *responsible for their own health insurance*, and the remainder received health insurance through their parents or a third party. Similarly only 3.1% of respondents were responsible for all of their *annual personal expenses*, whereas 78.5% of respondents were not responsible for any of their expenses. Respondents averaged 3.2 on the *general self-efficacy* scale, indicating a fairly high level of self efficacy within the sample.

Technology Use and Expertise

Respondents averaged 7.3 years *Internet use*, with the most experienced respondent reporting 15 years of use. Concerning *web expertise* respondents had completed 6 tasks (at the top of "intermediate expertise"), with the

TABLE 14.4
Descriptive Statistics for Individual Items,
Scales and Subscales, With Reliabilities

Demographics	*Min*	*Max*	*Mean*	*S.D.*
Gender M1F2	1	2	1.8	0.42
Age Years	17	28	19.5	1.39
Age Months	0	12	5.6	3.30
Healthy	1	7	5.1	1.25
Chronic Illness Y1N2	1	2	1.8	0.39
Annual Expenses Responsible for	1	5	2.1	0.99
Health Insurance Coverage Responsibility Y1N2	1	2	1.9	0.27
College Year 1F4S	1	4	2.0	0.84
Use of Internet Number of Years	2	15	7.3	1.91
Web expertise—sum of 12 items	0	12	5.99	2.26
Web expertise—grouped according to GT four levels of expertise: 0–3 activities, novice; 4–6, intermediate; 7–9, experienced; and 10–12, expert	1	4	2.34	.79
Web fluency α = .88	2.9	7.0	5.7	.82
Efficacy α = .86	2.1	4.0	3.16	.39
Need for Privacy α = .81	1.6	6.8	4.0	.78
General Privacy α = .66	3.5	7	5.8	.75
Organizational Privacy α = .85	2.6	7	5.5	.79
Organizational Collection Privacy 4.5 40.9% α = .67	2	7	5.1	1.1
Organizational Personal Privacy 1.3 12.2% α = .74	1	7	4.9	1.0
Organizational Unauthorized Access Privacy 1.2 10.5% α = .82	2.2	7	6.0	.87
General Concerns about Computer Privacy α = .88	1.7	7	4.7	1.2
Number of Accurate Patients' Legal Rights, out of 12	0	11	6.8	1.4
Relative Advantage α = .88	1.7	7	5.1	.84
Compatibility α = .78	1.4	7	4.7	.86
Complexity α = .69	2.1	6.5	4.4	.75
Error Complexity 2.3 32.9% α = .86	1	7	5.6	1.1
Explanation Complexity 1.8 25.3% α = .82	1	7	3.3	1.3
Trialability α = .77	1	7	5.8	1.1
Observability α = .64	1.9	7	4.6	.85
Adoption α = .88	1	7	4.2	1.1
Reinvention α = .89	1.3	7	5.3	.84

Note. $N = 403$–413; "α =" is Cronbach's alpha; *x.x* and *y.y*% are eigenvalue, and percent variance explained, respectively, for principal components analysis of subscales.

least completed task being "Bought a book to learn more about the Web or Internet" and the most completed task being "Ordered a product/service by filling out an online form." When asked how frequently they used the Internet from five different *locations*, the most popular place was respondents' homes, followed, respectively, by the library, school, other places, and work. On average, respondents reported a *web fluency* score of 5.7, indicating that most people were at least comfortable in completing the majority of the described tasks. Respondents were most comfortable with such basic web skills as "Using search engines such as Google or Yahoo," and "Using 'back' and 'forward' in your browser to return to pages." The tasks respondents were least comfortable with included "Creating a website using a visual editor," and "Creating a website using HTML."

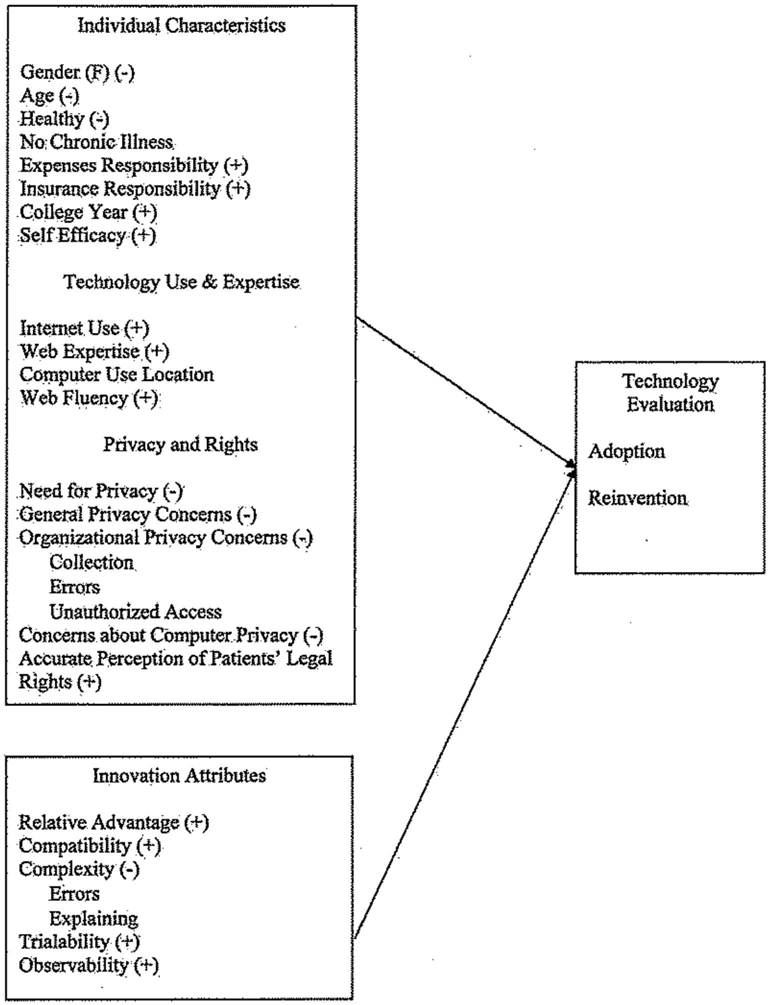

FIG. 14.1. Explanatory model of influences on DMR adoption.

Privacy and Rights

Respondents did not have a great *need for privacy*, averaging 4, and the area they were most concerned with was personal space. Respondents expressed greatest concern on the items "If I kept a diary, I would never show it to anyone," and "When working or studying, I need lots of elbow room." In contrast, respondents were least concerned with issues of concealment, such as needing to tint car windows or keep shades closed while in their homes.

General privacy concerns had a mean of 5.8, suggesting a fairly high level of concern. Respondents agreed most strongly with the statement "No one should be able to gather or disclose my personal information without my consent." On the contrary, respondents were least in agreement with the statement, "The government should be able to secretly monitor individuals' online activities for national security." The mean of respondents' *organizational privacy concerns* was 5.5, indicating a medium level of concern, with greatest concern about unauthorized access. For example, respondents most strongly agreed with the statements "Companies should never sell the personal information in their computer databases to other companies." Following unauthorized access, respondents were also concerned with the collection of personal information and errors, respectively. Overall, respondents' concerns about *computer privacy* were not as great as their general or organizational privacy concerns, with a mean of 4.7, slightly above "somewhat concerned." Respondents were most concerned with "getting a computer virus attack" and least concerned with "your e-mail will be read by someone besides the person you sent it to."

Respondents' averaged only 6.8 correct responses to 12 statements about *patients' legal rights*. The items respondents scored poorly on concerned physicians' and health care providers' abilities to share medical information without consent, demonstrating that respondents believed they had greater control over their medical information than is actually true.

Innovation Attributes

DMRs' *relative advantage* (compared to paper medical records) had a mean of 5.1, somewhat favorable. Respondents felt that DMRs' most advantageous characteristics were the records' availability in a emergency situations and the added convenience for doctors. The only statement that received below a neutral level of agreement involved DMRs' ability to save people money in comparison to paper records. *Compatibility* had a mean of 4.7, indicating that respondents at least somewhat agreed with the majority of statements. The statement receiving the highest score was "The individual patient should decide who has the authority to view the information in his or her medical record," whereas "My digital medical record would remain private" received the lowest level of agreement. In terms of *complexity*, DMRs were perceived to be most complex in susceptibility to both human and computer error, and respondents felt slightly more comfortable in their ability to understand or explain the technology. Respondents tended to agree with statements indicating DMRs' *trialability*, averaging 5.8. Respondents most agreed they would like the option to remove their medical record from the system in the future. The mean for *observability* was 4.6, indicating basic recognition of DMRs' observability. Respondents agreed most strongly with statements of action, such as viewing a list of those authorized to view their medical record, and less strongly with statements of support, such as their willingness to participate in a community forum on DMRs.

Technology Evaluation

On average, respondents agreed with statements of *adoption* with a score of 4.2, slightly above neutral. The statement with the highest level of agreement was "I would access my digital medical record if given the opportunity," and the lowest level of agreement was "I would participate in a consumer oversight committee to advise health administrators about recommendations for the SBCCDE." Respondents averaged 5.3 on the *reinvention* scale; respondents were most likely to agree with instances of patient reinvention (e.g., they would use their medical records to learn their medical history), and slightly less likely to agree with instances of doctors' and others' reinvention of DMRs, respectively.

RESULTS: BIVARIATE AND MULTIVARIATE

The overall model (Fig. 14.1) proposed directional predictions of individual characteristics, technology use and expertise, privacy and patients' legal rights, and innovation attributes' influences on an individual's likelihood to adopt and reinvent DMRs. Table 14.5 presents correlations between the variables—separate individual characteristics, and scales and subscales of *technology use* and *expertise*, *privacy* and *medical rights*, and innovation *attributes*—and the two outcome measures of *adoption* and *reinvention*. The bivariate analysis provided support for several of those predictions.

Multiple regressions were run to identify unique explanatory variance in adoption and reinvention explained by the variables, because of possible intercorrelations among the explanatory variables. All of the scales,

TABLE 14.5
Correlations of Explanatory Influences
With Adoption and Reinvention

Explanatory Influences	*Adoption*	*Reinvention*
Individual Characteristics		
Gender	–.08	–.05
Age total months	.01	.00
Healthy	–.06	.02
Chronic Illness	.00	–.03
Annual Expenses Responsible for	.10*	.11*
College Year	–.00	.01
Health Insurance Responsibility	–.11*	.01
General Self-Efficacy	.06	.17**
Internet Use and Expertise		
Internet Use	.04	–.02
Web Expertise sum	.09*	.13**
Web Fluency	.18**	.19**
Privacy Concerns and Medical Rights		
Personal Privacy Needs	–.02	–.02
General Privacy Concerns	–.01	.16**
Organizational Policy	.06	.22**
Concerns about Computer Privacy	.14**	.16**
Patients' Medical Rights #correct	.08*	.04
Innovation Attributes		
Relative Advantage	.47**	.41**
Compatibility	.49**	.32**
Complexity	–.19**	–.01
Trialability	–.07	.22**
Observability	.54**	.47**

Note. $^{*}p < .05$ level; $^{**}p < .01$ level (1-tailed). $N = 402–413$.

subscales, and individual measures with significant bivariate correlations were included, stepwise within three blocks (individual characteristics, privacy concerns and medical rights, and then innovation attributes). About 40% of the variance in adoption and a third of the variance in reinvention of the SBCCDE system was explained.

Adoption and *reinvention* of DMRs were significantly influenced by the percentage of annual expenses respondents were responsible for. No Internet use or expertise were significant influences on adoption or reinvention. The *collection* subscale of organizational privacy concerns and concerns about computer privacy were significant influences on adoption. The *unauthorized access* subscale of organizational privacy was a significant influence on reinvention. *Observability*, *compatibility*, *trialability*, and *explanation complexity* were significant influences on adoption. *Relative advantage*, *observability*, and both *explanation complexity* and *error complexity* were significant influences on reinvention.

TABLE 14.6
Final Summary Multiple Regressions
Explaining Adoption and Reinvention

Explanatory Influences	*Adoption*	*Reinvention*
Individual Characteristics		
Annual Expenses	.08*	.10**
Privacy Concerns and Medical Rights		
Organizational privacy—collection	–.12**	—
Organizational privacy—unauthorized access	—	.12**
Concerns about computer privacy	.10*	—
Innovation Attributes		
Relative advantage	—	.17***
Observability	.44***	.32***
Compatibility	.25***	—
Trialability	–.13***	—
Complexity—explanation	–.12**	–.16***
Complexity—error	—	.15***
Adjusted R^2	.41	.33
F-ratio	40.5***	32.8***
N	393	394

Note. $^{*}p < .05$; $^{**}p < .01$; $^{***}p < .001$.

DISCUSSION AND IMPLICATIONS OF SURVEY RESULTS

Individual Characteristics

The percentage of *annual expenses* that individuals were responsible for was the most significant individual characteristic related to both adoption and reinvention, whereas other characteristics, such as age and health status, were not significant. Responsibility for *health insurance* and *self efficacy* were also related to adoption, although their influence was not as prominent, and disappeared in the regressions. These results imply that those individuals with a heightened awareness of their financial obligations, such as health insurance, may be more likely to see benefits in

DMRs, and subsequently adopt the technology. Also, financially responsible respondents may possess greater *self-efficacy* as a result of their ability to maintain a sustainable income, and consequently may feel more confident in their personal ability to understand and use their DMRs. Therefore, when introducing DMRs to the public, it may prove useful to identify community segments according to financial independence, and develop programs to foster understanding of the new technology according to each group's specific needs. In general, materials presenting and emphasizing different aspects of DMRs should be developed in anticipation of a diverse consumer population.

Internet Experience and Expertise

Respondents who scored higher on measures of *web expertise* and *web fluency* were more supportive of DMRs and their own ability to successfully use the application, although both disappeared as unique influences in the regressions. Although the current study's sample of college respondents averaged 7.3 years of Internet use, such familiarity with the Internet may not be representative of other populations. For example, as focus group participants and SBCCDE stakeholders voiced, those community members with lower technology expertise will not be able to take advantage of DMRs, and, as the survey results demonstrate, may be less likely to adopt DMRs. To combat the large obstacle of deficits in computer skills among different segments of the population, whether they are senior citizens, minorities, or low-income families, regional health infrastructure organizations (RHIOs), such as the SBCCDE, may consider outreach programs to introduce people to the Internet. Indeed, the first of three primary recommendations by the Working Group on Policies for Electronic Information Sharing Between Doctors and Patients (2004) was to increase public understanding of the value of connectivity in health care through a coordinated, public–private communications campaign.

Also, as many RHIOs are concerned with establishing stable funding for their projects, continued community outreach, in terms of education programs introducing increasingly sophisticated technology into the community, may further their ability to obtain grants, federal funding, and overall public support. Disparities in computer skills should also be taken into consideration when developing materials or publications explaining DMRs and the SBCCDE. Although a discussion of peer-to-peer technology may reassure computer technicians that DMRs are secure, populations less web-fluent would most likely be confused and turned off to DMRs. Those groups whose fall toward the middle of the technologically savvy spectrum may benefit from a simple explanation of the

technology that utilizes analogies of web terms and functions with which they are more likely to be acquainted.

Privacy Concerns and Medical Rights

Respondents with a more accurate perception of *patients' legal medical rights* were more likely to adopt DMRs, but this influence disappeared in the regressions. Respondents averaged only 6.8 correct responses out of 12 statements regarding patients' legal rights, demonstrating that these college students were largely misinformed about their medical rights. This may well be true of most population segments, so any implementation of DMRs needs to take into account that consumers' concerns about new health technologies may be confounded by inaccurate assumptions about their actual medical rights. The SBCCDE should consider taking steps toward educating their potential consumers regarding their medical rights as mandated under HIPAA, and the manner in which the CDE strictly complies with those rights. Developing informative pamphlets, presentations, or videos for patients, constructed in a patient-friendly format avoiding legal and medical jargon, may facilitate consumer education. Also, as doctors are often seen as credible authority figures, it may be helpful to have doctors discuss medical rights with their patients, both privately in their offices and publicly in community forums, to reinforce the information and clarify any questions patients may have. Finally, Santa Barbara County, like much of California, has a large Latino population, and it would be wise to have all patient education materials available in both English and Spanish.

Concerns about computer privacy and the *collection aspect of organizational privacy* concerns were also related to the adoption of DMRs. Respondents with lower levels of privacy concerns were more likely to adopt the technology. Similarly, *general privacy concerns*, *concerns about computer privacy*, and the *unauthorized access aspect of organizational privacy* were related to reinvention. The relationship between organizational privacy concerns to both outcome measures points to the value of future efforts to establish stronger patient–organization relationships, whether it be through the organizations' outreach into the community, or other means that increase the visibility and accountability of the organization within the community. In creating a consumer education program, it might be helpful to explicitly address those issues respondents were especially uncomfortable with, such as the sale of personal information to other companies, the use of personal information for reasons other than stated, or the use of personal information without obtaining consent. Addressing consumers' specific concerns in a privacy pamphlet or video describing exactly how and for what purposes patients' medical information will and will not be used, might reduce consumers' privacy concerns. Also, it may be helpful to inform consumers about how they may engage in 'safer web practices;' for example, learning to look for Web sites' privacy policies and eliminating cookies from the hard drive. By educating consumers on how to better protect themselves from what they consider to be privacy violations, their self efficacy may increase and overall privacy concerns may be reduced, leading to the greater likelihood of adoption of DMRs.

Innovation Attributes

The innovation attributes were, out of all variables, the most strongly related to both outcome measures. In the case of *adoption*, *observability*, *compatibility*, *trialability*, and the *explanation* aspect of complexity were the most significant influences.

Relative advantage, *observability*, and the *explanation* and *error aspects of complexity* were significantly related to *reinvention*. Whereas *relative advantage* did not play as significant a role in adoption, respondents who saw significant benefits of DMRs in comparison to paper medical records were more likely to acknowledge various reinventions of the new technology. Therefore, in developing consumer strategies, the SBCCDE would benefit from enumerating the differences between DMRs and paper records, and by presenting the paper records as outdated or inefficient. Respondents reacted most positively to advantages focusing DMRs' abilities to enable better health care, especially by facilitating care in emergency situations, providing convenient information access for doctors, and by alleviating the pains of transferring paper records between physicians' offices and medical clinics. Such a focus on treatment is a positive result for the SBCCDE, as it reaffirms its stated dedication to improving health care by facilitating access to medical records at the point of patient care. Creating a variety of opportunities for individuals to interact with their DMRs, such as viewing a list of users authorized to view their record, will help them view the technology as compatible with their everyday needs and values.

REFERENCES

Albisser, A., Albisser, J., & Parker, L. (2003). Patient confidentiality, data security, and provider liabilities in diabetes management. *Diabetes Technology and Therapeutics, 5*(4), 631–640.

Alpert, S. A. (2003). Protecting medical privacy: Challenges in the age of genetic information. *Journal of Social Issues, 59*(2), 301–322.

Aydin, C. E., & Rice, R. E. (1991). Social worlds, individual differences, and implementation: Predicting attitudes toward a medical information system. *Information & Management, 20*, 119–136.

Bandura, A. (1997). *Self-efficacy: The exercise of control.* New York: Freeman.

Brewin, B. (2005). Public wants open health records standards. *Government HealthIT, June 3.* Retrieved July 21, 2005, from http://www.govhealthit.com/article89070-06-03-05-Web

Bunz, U. (2004). The computer-email-web (CEW) fluency scale: Development and validation. *International Journal of Human–Computer Interaction, 17*(4), 477–504.

Buss, A. (2001). *Psychological dimensions of the self.* Thousand Oaks, CA: Sage.

California HealthCare Foundation. (1999). Medical privacy and confidentiality survey: Summary and overview. January 28. Retrieved October 14, 2004, from http://www.chcf.org/documents/ihealth/survey.pdf

Care Science, Inc. (2005). *Santa Barbara County Care Data Exchange.* Retrieved July 21, 2005, from www.Carescience.com

Chin, T. (12 March, 2001). Peer to peer: Sharing patient data online. *American Medical News*, 1–6.

Committee on Information Technology. (1999). *Being fluent with information technology.* Washington, DC: National Academy Press.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189–212.

Connecting for Health. (2003, June). *Personal health working group survey.* Retrieved July 21, 2005, from http://www.connectingforhealth.org/resources/phwg_survey_ 6.5.03 .pdf

Connecting for Health. (2005, January). *The collaborative response to the ONCHIT* [Office of National Coordinator for Health Information Technology] *request for information.* Retrieved July 21, 2005, from http://www.connectingforhealth.org/resources/collaborative_response/collaborative_response.pdf

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115.

Davis, F. (1993). User acceptance of information technology: System characteristics, use perceptions and behavioral impacts. *International Journal of Man–Machine Studies, 38*, 475–487.

Demiris, G., & Eysenbach, G. (2002). Internet use in disease management for home care patients: A call for papers. *Journal of Medical Internet Research, 4*(2), 6–12, e6.

Epstein, R. A. (2002). HIPAA on privacy: Its unintended and intended consequences. *Cato Journal, 22*(1), 13–32.

Fedorowicz, J., & Ray, A. W. (2004). Impact of HIPAA on the integrity of healthcare information. *International Journal of Healthcare Technology & Management, 6*(2), 142.

Ferris, N. (2005a). Regional health information networks gain traction. *Government HealthIT, June 9.* Retrieved July 21, 2005, from http://www.govhealthit.com/article89134-06-09-05-Web

Ferris, N. (2005b). Health nets seek sound financial footing. *Government HealthIT, June 9.* Retrieved July 21, 2005, from http://www.govhealthit.com/article89146-06-09-05-Web

Finkelstein, J. B. (9 August, 2004). HHS outlines plan to increase national adoption of health information technology. *American Medical News.* Retrieved December 2, 2005, from http://www.hhs.gov/news/press/2004pres/20040721.html

Fuller, T. D., Edwards, J. N., Vorakitphokatorn, S., & Sermsri, S. (1993). Using focus groups to adapt survey instruments to new populations: Experience from a developing country. In D. L. Morgan (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 89–104). Thousand Oaks, CA: Sage.

Georgia Tech's GVU's 10th WWW user survey. (1998). Retrieved July 16, 2003, from http://www.gvu.gatech.edu/user_surveys/survey-1998-10/

Gunter, T. D., & Terry, N. P. (2005). The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions. *Journal of Medical Internet Research, 7*(1), e3.

Harris Interactive. (2003). eHealth's influence continues to grow as usage of the Internet by physicians and patients increases. *Health Care News, 3*(6), 1–7.

Hassol, A., Walker, J. M., Kidder, D., Rokita, K., Young, D., Pierdon, S., Deitz, D., Kuck, S., & Ortiz, E. (2004). Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. *Journal of the American Medical Informatics Association, 11*(6), 505–513.

Health Privacy Project. (2004). *HIPAA privacy check-up*. Washington, DC: Author.

Jeffords, M. J. (1999). Confidentiality of medical information: Protecting privacy in an electronic age. *Professional Psychology: Research and Practice, 30*(2), 115–116.

Jerusalem, M., & Schwarzer, R. (1992). Self-efficacy as a resource factor in stress appraisal processes. In R. Schwarzer (Ed.), *Self-efficacy: Thought control of action* (pp. 195–213). Washington, DC: Hemisphere.

Johnson, B., & Rice, R. E. (1987). *Managing organizational innovation: The evolution from word processing to office information systems*. New York: Columbia University Press.

Joustra-Enquist, I., & Eklund, B. (2004). SUSTAINS: Direct access for the patient to the medical record over the Internet. *MEDINFO 2004*(CD), 1673.

Knodel, J. (1993). The design and analysis of focus group studies: A practical approach. In D. L. Morgan (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 35–50). Thousand Oaks, CA: Sage.

Krueger, R. A. (1993). Quality control in focus group research. In D. L. Morgan (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 65–85). Thousand Oaks, CA: Sage.

Li, J., & Shaw, M. J. (2004). Protection of health information in data mining. *International Journal of Healthcare Technology & Management, 6*(2), 210.

Mandl, K. D., Szolovits, P., & Kohane, I. S. (2001). Public standards and patients' control: How to keep electronic medical records accessible by private. *British Medical Journal, 322*, 283–287.

McGee, M. K. (3 November, 2003). Collaborate and conquer. *InformationWeek*.

Metzger, M., & Docter, S. (2003). Public opinion and policy initiatives for online privacy protection. *Journal of Broadcasting & Electronic Media, 47*(3), 350–374.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35.

Morgan, D. L. (Ed.). (1993). *Successful focus groups: Advancing the state of the art*. Thousand Oaks, CA: Sage.

Muller, M. L., Burkle, T., Irps, S., Roeder, N., & Prokosch, H. U. (2003). The diagnosis related groups enhanced electronic medical record. *International Journal of Medical Informatics, 70*(2–3), 221–228.

Nasser, C., & Alpert, S. (1999). *Protecting the privacy of medical records: An ethical analysis*. Lexington, MA: National Coalition for Patient Rights.

O'Brien, K. (1993). Improving survey questionnaires through focus groups. In D. L. Morgan (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 105–117). Thousand Oaks, CA: Sage.

PC Magazine. (September 26, 2001). *A healthier CHIN*. Ziff Davis Publishing, Inc.

Ralston, J. D., Revere, D., Robins, L. S., & Goldberg, H. I. (2004). Patients' experience with a diabetes support programme based on an interactive electronic medical record: Qualitative study. *British Medical Journal, 328*(7449), 1159.

Reynolds, S. (2003). Making sense of information technology. *British Journal of Midwifery, 11*(3), 178–183.

Rice, R. E., & Anderson, J. G. (1994). Social networks and health care information systems: A structural approach to evaluation. In J. Anderson, C. Aydin, & S. Jay (Eds.), *Evaluating health care information systems: Methods and applications* (pp. 135–162). Newbury Park, CA: Sage.

Rogers, E. M. (1983). *Diffusion of innovations* (3rd ed.). New York: Free Press.

Shoesmith, J. (2001). Privacy matters: As the healthcare sector and high-tech worlds converge, governments and service providers are scrambling to ensure that the benefits of ehealth don't come at the expense of personal privacy. *Canadian Healthcare Manager, 8*(2), 21.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.

Swartz, N. (2004). A prescription for electronic health records. *Information Management Journal, 38*(4), 20.

U.S. Department of Health and Human Services. (2000). 45 CFR Parts 160 and 164. Standards for privacy of individually identifiable health information; Final rule. *Federal Register, 65*, 82462–82829.

U.S. Department of Health and Human Services. (2001). *Fact sheet: Protecting the privacy of patients' health information. July 6*. Retrieved February 10, 2005, from http://www.hhs.gov/news/press/21001pres/01fsprivacy.html

U.S. Department of Health and Human Services. (2004). *OCR letter to healthcare providers*. May 17. Washington, DC: US DHHS Office for Civil Rights.

Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information Management and Computer Security, 9*(4), 165–174.

Wang, M., Lau, C., Matsen, F. A. III, & Kim, Y. (2004). Personal health information management system and its application in referral management. *IEEE Transactions on Information Technology in Biomedicine, 8*(3), 287.

Wang, S. J., Middleton, C., Prosser, L. A., Bardon, C. G., Spurr, C. D., Carchidi, P. J., Kittler, A. F., Goldszer, R. C., Fairchild, D. G., Sussman, A. J., Kuperman, G. J., & Bates, D. W. (2003). A cost-benefit analysis of electronic medical records in primary care. *The American Journal of Medicine, 114*, 397–403.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, 4*, 193–220.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Williams, F., Rice, R. E., & Rogers, E. M. (1988). *Research methods and the new media*. New York: The Free Press.

Wolff, B., Knodel, J., & Sittirari, W. (1993). Focus groups and surveys as complementary research methods: A case study. In D. L. Morgan (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 118–136). Thousand Oaks, CA: Sage.

Working Group on Policies for Electronic Information Sharing Between Doctors and Patients. (July, 2004). *Connecting Americans to their healthcare. Executive summary*. Retrieved July 21, 2005, from http://www.connectingforhealth.org/resources/eis_exec_sum_final_0704.pdf

Ziebland, S., Chapple, A., Dumelow, C., Evans, J., Prinjha, S., & Rozmovits, L. (2004). How the internet affects patients' experience of cancer: A qualitative study. *British Medical Journal, 328*(564).