Consumer Control of Electronic Personal Health Information: What Does It Mean? Why Is It Important?

A Report on Three Consumer Focus Group Meetings Convened in October, 2005 by the Office of the Assistant Secretary for Planning and Evaluation

Susan Kanaan
Independent Consultant

Suzie Burke-Bebee, MSIS, MS, RN
Helga E. Rippen, MD, PhD, MPH
U.S. Department of Health and Human Services

March 1, 2006
Prepared for
Office for Science and Data Policy
Office of the Assistant Secretary for Planning and Evaluation
Department of Health and Human Services
Contract #HHSP23320045014XI

—Contents—

Consumer Control of Electronic Personal Health Information: What Does It Mean? Why Is It Important?

A Report on Three Consumer Focus Group Meetings Convened in October, 2005 by HHS/ASPE

"I think what this HIT movement will do is really validate us as partners with our medical providers—and not just as being receiving care, but actually participating."……Anonymous Participant

Introduction

Public and private health care sectors recognize that health information technology (HIT) plays a pivotal role for improving health care quality while reducing health care cost. Many new initiatives have created a momentum greater than in the past for adopting electronic health records (EHRs) and HIT in general. In the current environment, the principle that the patient and consumer control their personal health information (PHI) is frequently invoked and linked to the broader principle of patient-centricity. Surveys by the Markle Foundation and the California Health Care Foundation confirm that most consumers are concerned about the privacy and security of their PHI. While many consumers recognize the benefits of EHRs and other forms of HIT, they want and expect to control access of their PHI—who sees it, what they see and under what conditions.

Several organizations such as the Consumers Union, Health Privacy Project, and National Consumers League support a set of consumer-focused principles for designing a nationwide electronic health infrastructure[1]. An immediate challenge persists in defining what control means to the consumer and soliciting consumer engagement in workable solutions as the industry plans for HIT implementation. To this end, the Office of the Assistant Secretary for Planning and Evaluation (ASPE) within the Office of the Secretary at the Department of Health and Human Services

[1] Markle Foundation response to the Office of the National Coordination for Health Information Technology for a request for information (RFI), January 18, 2005. On-line access: http://www.ahqa.org/pub/uploads/Day_2_Track_6_Consumer_principles.doc

hosted three consumer focus group meetings in October 2005 for day-long discussions on these topics. Health Services Research and Shugoll Research recruited the participants.

This report makes no attempt to associate the participants' opinions with any individual characteristics. Apart from the fact that most participants lived in the Washington, D.C. metropolitan area, the diversity of the participants included ages ranging from the twenties to the seventies; a broad socioeconomic and cultural background; and a wide range of jobs and professions. A few were students, and most, though not all, live with serious or chronic physical or mental health conditions, either their own or that of a close family member—including psychiatric disorders, breast cancer, multiple sclerosis and HIV. At least one person in each group serves as a peer counselor for consumers with whom they share a health condition enriching their life experiences. The variety of the participants' life experiences contributed to lively discussions all three days with many work and health-related experiences providing valuable anecdotal illustrations.

One characteristic found with little variation: the participants' intense awareness of their medical and health records and the lengths to which many have gone to access, compile and maintain them. One person actively uses electronic personal health records for herself and her son; others use a variety of paper-based systems, including a Rolodex, filing systems, and lists of medications and immunizations. A few participants access PHI through their health care providers' EHRs. Several described the convenience and comfort of knowing their complete records were in one place following them from physician to physician inside their HMO or in the Veterans Administration health care system.

Hurricane Katrina, which wreaked havoc just seven weeks before these discussions, provided a strong reference point for all the focus groups. Among other lessons, the catastrophe reinforced the importance of health records especially the vulnerability of paper records. One of the three media articles[2] sent as background material for the

[2] Jonathan Krim, "Health records of evacuees go online," *Washington Post*, September 14, 2005. This and the other articles are in Appendix B.

participants prior to meeting described the efforts by the federal government and others to reconstruct evacuees' medical and pharmaceutical records making them available to health care providers online.

Groups of nine, twelve and eight participants met on October 17, 19 and 21 respectively at Shugoll Research in Bethesda, MD, for six hours of discussion (each) with their facilitator, Larry Bartlett, PhD, from Health Systems Research, and Helga Rippen, MD, PhD, from ASPE. The participants sat around a large table in a special focus group room. Dr. Bartlett made the participants aware of a two-way mirror and the handful of observers in an adjoining room. He encouraged them to speak about their own experience and to imagine how other experiences and conditions (e.g., a personal or family health crisis) might affect their views. In addition, Dr. Bartlett encouraged them not to worry about reaching agreement on any of the topics or issues. The intent of the focus group discussions was to explore a full range of views on every subject with "no wrong answers."

To provide context for the discussions, Dr. Rippen briefly described the challenges of the current health system and the improvements proposed by federal policy makers and the health care industry through implementing electronic health records (EHRs) and HIT. She discussed the Nationwide Health Information Network (NHIN) as a valuable tool for improving safety, reducing costs, managing public health threats and supporting research. Dr. Rippen cited the potential benefits for consumers and physicians, making it possible to share health information any time and any place. Finally, she stressed the need to actively engage consumers for their perspective in resolving the issues of how to control electronic sharing of their personal health information.

This brought each of the groups to the focal topic—exploring what control of PHI means to these consumers. After encouraging reaction to Dr. Rippen's introduction, Dr. Bartlett led each group in informal discussions on topics covered through a prepared outline of questions (Appendix A). The discussions generally followed the structure of the questions with enough flexibility for the groups to carry the topics in directions that interested them with Dr. Bartlett ensuring that all the topics were

eventually covered. Like the discussions themselves, this report attempts to capture the full range of views, moving from general impressions to a series of specific topics and back again to the participants' broad concluding comments. Due to the insightfulness of the participants, many individual voices are included in sidebars to give a sense of the richness of the discussions and the variety of views expressed. The quotations loosely parallel the narrative and may be read in tandem with it.

1. First Impressions

To begin the discussions, the facilitator invited responses to Dr. Rippen's introductory remarks. In particular, Dr. Bartlett asked the participants to share their initial thoughts about the potential benefits and risks of electronic PHI, the pivotal notion of control, and how much control they have at present.

a. Potential benefits and risks of electronic health records and systems

It is obvious that the technology we are using in health care today is about 100 years behind the rest of most of the other things in technology. So I do see tremendous potential benefit. Of course, there are also all these problems.

The initial comments laid out a number of issues and themes that each group explored in greater depth over the course of the day-long discussions. The comments revealed a wide range in attitudes toward the anticipated benefits and risks of electronic PHI and the tradeoffs between them.

I am a parent of children with special healthcare needs. You go from specialist after specialist after specialist, and I'm tired of telling the whole record every time, from the diagnosis all the way through.

Most participants easily recognized potential benefits and risks with electronic PHI. The named benefits included:

- having all my children's doctors see the same information;
- getting to see my test results promptly;
- having access to my elderly mother's PHI so I can advocate for her more effectively;
- having all my health information quickly accessible to health care providers in an emergency;
- improving my physician's ability to communicate with other health care providers;
- being able to see and change misinformation in my record;
- ensuring that my records would survive a fire, flood or other natural disaster;
- making it easier to compile my health records;

I've had the experience of going to my physicians and having them be able to immediately look on, pull up my most recent lab work and say, 'Oh, yeah.' Right there, at that [visit], we could decide, no, you don't need the lab work, and so I think it is wonderful.

- avoiding unnecessary tests;
- transferring records to new doctors more easily;
- not needing to remember all my medications;
- avoiding dangerous drug-drug interactions;
- receiving more complete, round-the-clock health care services for me and my family; and
- improving public health programs and medical research through better statistics.

I would get at it from the perspective of all the recent Katrina victims. They have no medical records now, nothing. Just one thing can happen, a fire or anything could happen, and your records are gone.

The participants identified personal and societal benefits from electronic health information. These benefits include the ability to better manage their own health and that of family members, greater convenience, improved health care, and stronger research and public health programs. One participant with an EHR spoke about her peace of mind knowing her complete personal and family records were in one place within her HMO. She looks forward to easier access in the future through a new feature being provided: a personal web portal.

Will they make it possible that every time we go to the hospital, you don't have to tell them what medication you are taking and then they ask you 100 times?

When naming risks, most participants expressed fear that the wrong people would get hold of their personal information and use it against them. A few people described the risks as so serious it deterred them from wanting to be a part of an electronic system. Most participants looked at the risks as problems that could be solved through careful planning, consumer participation and informed public policy.

It is wonderful to have that information available, but who is going to control it, and are we going to be penalized for it? I think as we move forward, we really need to look at that.

From the outset, the idea of electronic interconnectivity in the health care system was especially sensitive. Many expressed extreme discomfort with the idea of their PHI traveling outside the walls of their health care organization and ending up "…in an Internet-type Web that everybody can

The freestanding electronic record, how the doctors get the information—that is different than putting it in an Internet-type web that everybody can get to.

get to." While a few participants pointed to the greater benefits of EHRs when interconnected, many wanted to mitigate the risks by limiting access to within the walls of their own health care organizations.

For a few participants this limitation was not enough. They preferred paper records, which they saw as easier to manage and control, possibly the only way to assure control. And regardless of PHI on paper or within EHRs, many expressed a strong mistrust of government and commercial interests. Some cited concerns about hackers. Others felt any assurances offered about consumers controlling access were meaningless and doubted that consumer control was technically possible regardless the intentions of policy-makers.

My big concern with an electronic health record is what sort of protections would be there to prevent these records from being hacked into. The statement "Trust us, something would be absolutely secure," is not something I really believe in.

I think it's absolutely a waste of time, money, and it's completely ridiculous. I view my personal medical records as my property. I don't want them stored in a database with anybody else's; I will keep them myself. And I really think mandating any sort of system like this would be completely anti-American.

Hesitation in seeing the value of electronic PHI related to the participants' views of any new technology. Many believed that early EHR implementation may be flawed in the area of security protections. Opportunists may exploit gaps in consumers' privacy protections in the early stages. One person noted the typical lag between abuses and protective laws and regulations making the case that protections are typically instituted *in response* to abuses, not prior to them.

In my personal opinion, our information is there, and we think it's safe, but at the end of the day, there are people going and grabbing whatever information they need. How can we assure that the consumer truly has 100 percent control? They have easier ways to get in there and get it because now it's on the system. It's like they eliminate us as the middle man. They can just get it without asking us.

Several participants raised issues about the future of the health care system and social equity. For example, one worried that uncoordinated implementation and a lack of interoperability (i.e., the ability to exchange meaningful information) in electronic systems would result in even greater fragmentation in the health care system. Several people expressed concern about whether everyone would benefit equally from health information technology. Various

comments pointed to disparities related to insurance, physical and cognitive abilities, health literacy, and technology access (the digital divide). Others wondered if consumers would understand how to exercise their control and properly use the increased mass of information.

To summarize, the range of concerns and fears about electronic PHI included the following:

- losing my privacy;
- errors in my electronic health record;
- someone hacking into my PHI if it's in a centralized database;
- losing control of my PHI if I change health insurance companies or doctors;
- lack of consumer competency to handle medical information and to exercise control over access;
- exclusion of disadvantaged Americans from electronic systems (i.e., digital divide);
- less candor in the medical record because the doctor knows the patient will see it;
- my employer or insurance company using my health information against me;
- government taking liberties with my PHI, rationalizing that it's for collective benefit;
- consumer complacency because they think everything is being automated (for them).

Whatever their personal views about EHRs, several participants indicated that they knew the transition to electronic systems was already under way. With this recognition, and in view of the potential for human and technological error, many expressed hope that those in charge of the transition would take the risks seriously and do

everything possible to protect their PHI. Thought to be equally important, participants called for consumers to have a voice and a seat at the table in the policy development and implementation process—starting *now.* The theme of consumer engagement is explored further in the final sections of this report.

b. Notion of control

A pivotal question that emerged when discussing the balance between benefits and risks of electronic PHI was *who will control access to my personal health information.* Several participants made it clear that benefits would depend entirely on their ability to control access to their PHI.

Control means making decisions about who has access to my information, but also actually being able to see the information myself.

Personally, I spend or have spent an inordinate amount of time keeping track of my medical records, and frankly, I am exhausted from doing that.

Control has dual meaning for these individuals: first, improving the speed, convenience and completeness of access to their health information; and second, retaining choice about the access of others. People spoke of wanting access to their records for two reasons: to keep track of and manage their health, and to find and challenge any errors in their records. Most recognized their legal right to access their records, but described finding many obstacles in their way as they tried to exercise that right.

Just making people more accountable, following up with people's mistakes that they write about you. That's advocating for yourself. I don't have no problems with none of my doctors, but you have to make them accountable. The first mistake — take care of it right then and there.

The second perspective on control of electronic PHI—access by others—was a major focus of these discussions. Most took electronic PHI as a given, and went on to explore and refine their views on the variables involved in determining who has access, to what information, and under what conditions. One participant viewed the only meaningful control was to have the only copy of his medical records, which would also

In the packet of information that we got from you all, there was one quote that I think I underlined a hundred times that said, "If you can't control access, then you will start lying" — and that's so not in our best interest.

enable him to determine others' access by keeping the record at home and carrying it to medical encounters.

A few participants questioned whether genuine consumer control—meaning total, ongoing control—is actually possible in an electronic system. This question surfaced periodically during the three, day-long discussions. A variety of reasons for skepticism surfaced: the flaws and limitations in technology and security systems; the inability to keep control mechanisms simple; the inevitable lag between innovation and legal protections; and a possible unwillingness of policy-makers or health care providers to cede genuine control to consumers. A few expressed concerns about the cost of a complex system of control options.

I feel that as long as I keep control and I am responsible for it, I am going to have my own best interests at heart. If I have the only copy that exists of my medical record, I have the control, because no one else gets a copy unless they come through me. Once I have given the copy away I have lost control. The thing I like about paper is there it is, I have my hands on it, and you can see it: Okay, now I have control.

c. Consumer control now

When asked about how much control of their PHI they had under current conditions, they were well versed on the limits of their personal access to their records. Several people described past difficulties in seeing their records or getting specific information such as test results. They spoke of obstructive state laws, resistance by physicians or office staff to their requests for information, and the expense and inconvenience associated with getting their records. One called the common practice of charging for paper copies "an insult." Another person described the struggles of mental health consumers who may treat in multiple jurisdictions when getting copies of records. She explained how important it is for mental health consumers to have voluntary control over choosing to disclose their diagnoses.

In Virginia and D.C., you can only access your lab test results through your doctors. I got them to send me the records, but it's just a big headache.

First of all, more information is out there than you know.

Regarding their control of access by others, most people thought they had relatively little control under current conditions. One focus group, in an informal straw poll, rated their control of PHI at below 5 on a 1-10 scale (1 lowest, 10 highest). In another group, the only person to describe a high level of control over access was an HIV-positive participant who benefits from uniquely stringent privacy protections. While she values the protections, she described the current provisions as cumbersome and was an active proponent of electronic systems.

I have seen it at the Federal, State, and local levels. People will do the darnedest things. If they are going after tax records, well, you better believe they're going to go after health records.

Right now, I have a lot of control and that's good, but it's inconvenient. I have to go to all these places to do it.

Throughout these discussions, people would occasionally remind each other of the limitations of existing health information systems as they considered the apparent risks of electronic records in various contexts. For example, someone would point to a risk they associated with EHRs—such as employment discrimination—and someone else would observe that this risk already exists with paper records. The only counter-point in this comparison was that today, a person can go outside the system if willing to self-pay—as many do for HIV tests, for instance. People saw this as one form of control that may be lost if electronic records are consolidated across health care settings and providers.

I live in a very small town. Everybody talks. I go into the doctor's office, and they are all looking at your chart. So we actually are putting a higher standard electronically—and I agree with that.

I have felt like things I have said have ended up seeming very naïve, because someone else is saying they can already do that now. So is this like a totally worthless conversation? Will we really have any control, anyway? Do we really have the choice?

Many participants' thinking evolved over the course of the discussions regarding the question of current control. The more they talked about it, the more they viewed a lack of control today. One person observed that we have no idea who sees our records today. People began to consider electronic PHI as being more secure than paper because of enhanced technical abilities to manipulate and select data and create audit trails. In a follow-up straw poll, conducted in the context of possible new security measures, the same group

Under the new system, I could see, in a way, it could be better because you probably could have more control. Now, it's so easy to access and hard to prevent.

polled about current control of their paper records gave a higher rating to their anticipated control of PHI in electronic records.

2. On Controlling Access—The Details

After sharing their general impressions and initial thoughts about control, the focus groups progressed to a discussion about controlling PHI access in a more specific context: clinical and non-clinical settings; identified and de-identified health information.

a. Access within the health care continuum

There were as many opinions about the nuances of controlling PHI access in a clinical setting as participants. However, there was no variation in their determination to exercise control. In general, people want fairly liberal access to their PHI for health care purposes; but even then, many want constraints. The facilitator explained that control over access can be exercised in many ways: through who has access, the conditions under which access is allowed, the type of information, and the level of detail. (The participants later added duration of control to this list.). People generally felt it was necessary to discuss these variables together because of their interdependence. One example given was that a dermatologist and gynecologist did not need to see mental health records and vice versa.

For consumer control to have any real meaning, you have to be able to control instances outside the provider network where everybody could get to look at it. You choose to give permission and it needs to be a very narrow permission. The information needs to be controlled and not utilized except in the way that you wish it to be utilized by whoever you release it to.

To answer these questions, who, why, when, and what—it's very difficult. Each of them is contingent on other factors. Who I want to get information to depends on what information. What information depends on for what purpose.

One theme emerged in this context concerning the relationship between the values of control and quality of care. Some participants emphasized consumer control as a

way to improve quality by finding errors in their records and generally being more involved in their own health management. Others were more concerned about undermining the doctor-patient relationship. A few participants cautioned their fellow members against assuming any particular association between electronic records and quality of care. Several fallacies were pointed to: assuming electronic information was correct (several had found errors in their records); assuming physicians would read all PHI (some had received medication prescriptions to which the record had listed their allergies); and assuming EHRs assure provider competence (several told stories of poor medical judgment that had harmed them).

This is not the nirvana. You assume there is going to be clinical competence just because they are putting it into a computer. But in my experience, this is not necessarily so.

1. Access for whom — role-based access

Most participants wanted to put few, if any, restrictions on their primary care providers' access to their electronic PHI with an exception for when they moved to another doctor. The major premise was that the much valued doctor-patient relationship—which relies on information—must be protected. Participants want to make decisions about PHI access in partnership with their primary physicians, who could be a resource to explain various options.

If you get to a point where you have a good relationship with that physician, you should have that decision with the physician. They should be saying to you, "If you choose to disclose this information, this is how it is going to be used. This is the intention." It allows the consumer to ask questions. Then you can say yea or nay. That discussion definitely has to take place with the physician.

One person envisioned a form in which he could designate who had permission for access and who did not. He chose unlimited access for his primary care physician, specialists and emergency personnel; public health workers, social workers and trial lawyers would not have access. Another participant described her concern about ensuring all the right people *do* see the necessary information about her rather than about who should *not* see it.

I have a team of doctors. I want everyone on the team to know what's going on with me, particularly because I have very adverse reactions to certain types of medications. So one of my concerns is to be sure that the information gets to all the people I want it to. It's not just who doesn't have access, but it is also having a say over who does have access.

The prospect of emergency treatment was a clear example of the potential benefits of sharing electronic PHI for the participants. They recognized the advantages of having their information readily available to first responders and emergency room staff, and there was little disagreement about the appropriateness of this use "to save life and limb." One area of debate centered on whether emergency care providers should see a limited data set.

Back then I would go to different doctors, I wouldn't tell certain ones that I was HIV positive because it's not their business, but then it was like the side effects to the different medications. Now when I go to a doctor, that's the first thing I tell him, because I want them to be able to provide me with the best health that I can get for myself. And I am also starting to be a part of different clinical trials to help not only me, but to help that next person.

The focus groups also talked about what kind of access was appropriate for their providers' administrative staff. They generally agreed that office staff should only see the minimum necessary to carry out their responsibilities. One person asserted that people should trust their physicians to impose appropriate controls and protections in their offices and institutions. Another pointed out the practical difficulties of restricting access for different staff members in a physician's office, arguing instead for audit trails. In this area, as in others, many participants observed that electronic records could provide more protection for PHI than currently exists with paper.

I am just thinking how a medical office works. I think [creating audit trails] is very simple to do with an electronic health record, but to limit [access in a medical office] is going to be almost impossible. We are putting much higher standards, if you notice, on the electronic part.

2. Access under what conditions

In both clinical and non-clinical settings, the intended use of PHI can determine people's willingness to grant access to their PHI. In the clinical context, most people favored unrestricted access for routine care and either unrestricted access or a limited data set for emergency care. For second opinion consultations, several would like the ability to impose limits on what the "first opinion" physician knows about the consultation as well as what the consultant knows about the original opinion.

I will tell the surgeon, "Do not share any of my information to this second surgeon that I am going to for a second opinion."

Referring to new electronic prescribing policy, Dr. Rippen asked one group whether their physicians should be able to follow up with the pharmacy to find out whether they had filled prescriptions. The participants varied with their responses. Some pointed out that this information would be useful to the physician while others did not want their physician to have this information unless they chose to provide it.

3. Restrictions based on type of information

The idea of controlling specific types of health information accessible to health care providers such as sexual history, genetic test results, or psychiatric records, stimulated considerable discussion. As noted earlier, the focus groups included many individuals living with serious and chronic conditions and some who serve as peer counselors for others with their conditions. These multiple perspectives imparted richness and realism to the discussion of what information should be accessible, to whom, and under what conditions.

One problem I have run into is that doctors are often biased, and if they see any mental health record and you are being evaluated for physical symptoms, they may say, "It might be in your head, you are imagining or whatever it is." I would like to have the ability, when somebody is requesting some information, to ask them. "Why do you need this?" and to have them give me an explanation—to have an interactive system. Then maybe I'll say I wish to block my psychiatric records.

Many people want the right and ability to block access to specific types of information, even though they recognize the risks of withholding information and don't expect to exercise the right very often. They readily described scenarios in which they would not want certain things known about them, even in a health care setting. One participant cited bias that his psychiatric record might provoke in a physician treating him for a physical problem, thus he would block this information if not persuaded differently. Another would restrict access to family history such as sexually transmitted diseases (STDs) because it exposes another's personal information . In contrast, an HIV-positive participant had

I think physicians need broad access. For example, polypharmacy is a huge problem. How are the people that you go to in the emergency room going to know what is going on? If they haul me into the emergency room and I am unconscious, they need to know this stuff to care for me. I don't think even fairly sophisticated individuals are able to tell "this is going to be important to this doctor, and this is not going to be important to that doctor." That is why we've got experts.

learned that it was in her best interest to ensure that all her health care providers knew of her condition.

In general, the "need to know" principle proved useful when considering all issues about access. Group members experienced with security clearance introduced this principle.

With my security clearance, it's on a need-to-know basis. You may have the same clearance I have, but I do not need to know what project you are working on, therefore, I don't get that information, and I shouldn't have it—and if I do get it or try to get it, big penalties.

4. Consequences of withholding information from clinicians

The focus groups engaged in lively discussions about the pros and cons of withholding information from clinicians, with equally strong opinions on both sides. While several people expressed a desire to block access to some of their information (as seen above), others questioned the wisdom of doing so. The latter group argued that lay persons cannot possibly know what information will be needed to care for them, and that they could harm themselves by withholding. One person observed that blocking information "could be a matter of life and death." The statement "I'm not a doctor" was invoked more than once, along with questions about consumers' abilities to make good decisions on their own behalf. Some participants expressed practical concerns about making the system too complicated and costly by offering too many options. Others worried that withholding too much information could undermine the statistical validity of public health and research data.

The more I have listened to the discussion, the stronger I feel that we should err on the side of not blocking. Because you have to treat me, and if we choose to block information and then something happens to us and we don't get the best medical care, then we are responsible. I think we need to let the doctors be responsible and feel responsible. I feel so strongly, now that I have heard everybody.

I do feel like there is a certain integrity in the medical field, and that a lot of the talk and what is going on almost seems to change that. It is very bothersome to me.

I want all of this information there and easily accessible, so that the physician I see can look at everything and get a picture of me. Whether it's an emergency situation or it's my internist or my oncologist or my surgeon. By putting in blockings here and there, I am hampering their ability to take care of me in the long run. I see that as a bigger problem than somebody reading something.

The pivotal doctor-patient relationship was a persistent reference point in the focus group discussions. Most supported protecting this trusted relationship. Several people noted that withholding information could undermine provider relationships and even the quality of care.

One participant experienced with legal issues introduced the topic of physicians' risk management, stating he supports a doctor not accepting a patient who withheld or blocked information. Participants in all groups acknowledged that when information is withheld, the physician's liability decreases and the patient's responsibility increases.

As a matter of risk management [for physicians], if a patient comes in and says you can't see my whole medical record, you don't need that patient. Up front you explain to them if they have a question, "I really need to see everything because you really are not competent to make that decision," and if not, you don't need that patient. If you have people who want to keep secrets from you, can you properly treat them?

Several people stood firm for their right to withhold personal information, although not expecting to exercise it often. To help with such decisions, one person suggested that electronic records include a function alerting consumers to any possible harmful consequences of withholding information.

I don't want him necessarily to see the rest of my medical chart. I just want that right. —Not that I would use it, but I just want that right.

5. Levels of access, and limiting the duration of access

In the course of the day-long discussions, many analogies and examples proved valuable in probing the complex issues of PHI control. For example, one participant working with credit histories noted the parallels between EHRs and credit records. She explained the different levels of information available for checking people's credit under different conditions offering that similar levels of detail could be made accessible for PHI.

I am a little troubled by the idea that you can have levels of information—and I understand people's need for that; they don't want everyone else to have this. But what if you are in an emergency situation? You are hurting yourself because you are not providing the information. That is why they do the patient history in the first place and annoy you with all the questions, because they want to know that.

Most participants preferred allowing different levels of access, either dependent on the setting or the provider. Some preferred sharing a minimal data set of relevant PHI, such as to emergency personnel. One person, a strong proponent of standardizing health records, cited the World Health Organization's yellow immunization booklet as an example of a standardized "short form" for a narrowly defined purpose. He thought it would be useful to have a standardized list of all of his medications, to guard against harmful interactions.

Back then I would go to different doctors, I wouldn't tell certain ones that I was HIV positive because it's not their business, but then it was like the side effects to the different medications. Now when I go to a doctor, that's the first thing I tell him, because I want them to be able to provide me with the best health that I can get for myself. And I am also starting to be a part of different clinical trials to help not only me, but to help that next person.

Timing of shared PHI is another area of control valued by these consumers. Two options discussed: limiting the period of time health care providers have access to PHI, and giving consumers the ability to block access in the future. Participants' wanted enough system flexibility to allow them to change control settings periodically as their needs and circumstances changed.

Because of lack of information, they are not going to make the best decisions for me. If I say I want you to see this, but not this, then, if they hurt me in any way, it's partly my responsibility. I think it should be blanket access for any healthcare provider.

6. Access to self-entered information

Although only one person described personal experience with an electronic personal health record, most participants understood that consumers could create and maintain their own electronic health records—either in a separate document or in a protected area of the clinical EHR. The groups talked about the types of PHI they would record: a pain diary, weight and exercise, out-of area treatment, and complementary and alternative treatments.

If you are a highly allergic person or have other concerns and issues, it is to your best advantage to put that information in. Or you have lost 100 pounds in 6 months, and you are in an emergency room. That might be important to somebody treating you. The function should be there, though not everyone will use it. You should have the option to share or not.

The participants recognized the clinical utility of self-entered information. One observed that "when the doctor is really looking at you as a whole being," that doctor needs to have as much information as possible. Others noted the clinical significance of this information such as extreme weight loss, a new form of exercise, overseas travel, over-the-counter remedies, and pain or other symptom records. Operative criterion for what self-entered information to share with a physician was defined as what would contribute to the most effective health care. The participants agreed that self-entered information is the property of the person who entered it, and that individual should be able to block or share specific information with specific providers at his/her discretion.

Other perspectives on self-reported data questioned the reliability of such information, one participant joking that "…the Commonwealth of Virginia thinks I weigh 125 pounds!" Another described self-entered information as potentially harmful "noise" if included in the health information system.

I have personally known people who would have been terrified by the results of what physicians were finding. I don't think we can protect people from being scared. We have to treat them like adults and give them the information. I can't think of any better way. Otherwise, I or whoever is sitting in the big place is looking down and saying, "Well, you get to know, and you don't"—and that just doesn't fit with my image of where we live.

7. Access by individuals to all personal health information

The participants attach considerable importance to having access to their own personal health information. This emphasis on personal access, which emerged early in the discussions, resurfaced in response to a question about whether there was any medical information people should not be allowed to see. In other words, is there ever such a thing as *too much information*?

I tend to think that if you want the information and it's your information, then that's your responsibility, and you should have access to it.

A typical response was that while it is possible to imagine instances when people should not see their information—e.g., a disturbing or confusing test result—a more important principle is the right to see everything. Several participants linked this right to their responsibility for their own health and contended that people be treated like adults. Learning abnormal results should be tempered with a provider's good judgment, such as regarding timing and setting. Other unique circumstances should be handled through a designated proxy such as when a mentally ill patient experiences treatment for a psychotic episode. When asked whether people should have access to health information that employers or others collect about them outside a health care setting (e.g., drug test results), the groups favored complete access to this information.

I'd want to be able to designate one other family member in case, for some reason, I was incapacitated and couldn't speak up for myself. I would want to have someone on record who is related to me to have access to those records, so that they could make an informed decision.

8. Access by family members

Many participants shared the worry that family members would see their private health information. One described problems caused for him when a relative revealed sensitive information about him with others in his family. To restrict family members' access but ensure that someone had it in an emergency, the participants favored having a mechanism for assigning this right to a single designated proxy, as with a power of attorney.

You should be responsible for being able to make that decision, and that would need to be explained to the consumer: "Okay, you have absolute control. If you want to have somebody take care of you, if, God forbid, you become unconscious, then appoint somebody—and this is how you do it."

Family member access is a particularly complex issue for people with psychiatric disorders, a group that one member described as having unique concerns. This participant noted that many mental health patients pre-designate a proxy to manage their health information during episodes when they are cognitively impaired.

9. The idea of connectivity

The word "database" and references to a nationwide information network raised alarms for many participants. Most members of one focus group affirmed that the word "electronic" meant both a "centralized database" and "government" involvement. Connectivity evoked fear of diminished personal control as well as concern about hackers, stolen identities, "outsourcing to Singapore," and lost jobs or insurance.

Access is great if hackers didn't exist; but you can have your identity stolen. What is going to protect your medical records from being stolen, from being confused, -- a hacker could just have fun messing around. Nothing is safe on a computer. Did you see today's news? I don't want people to have a central access to my files. I do want my doctors to talk to each other—but through me. I can bring my records with me.

One focus group was asked to choose between having their PHI in an interconnected electronic system among providers, or keeping it separate, carrying their records at all times. Two-thirds want to be part of an interconnected system, and one-third want to avoid it.

In support of connectivity, for example, a parent of children with special needs spoke of the benefits for families like hers from government agency data-sharing on their children. It was noted that some benefits of EHRs, such as portability from doctor to doctor, depend on having an interoperable system. Some participants focused on the potential public health and research benefits from aggregated, de-identified electronic records (discussed further below).

I don't want possible insurers or employers going into them. I'm afraid of them being centralized because I think that you lose control when they are centralized. I am holding out for universal coverage before we have centralized records because I don't trust the insurance companies. They're just dying to deny us.

People's differing assumptions about two pivotal questions—whether real security is possible and whether consumers will be granted genuine control—were important in the context of interconnection. For example, while one person cited the relative security of credit records as an argument for trusting security measures, others called attention to media stories of publicly released PHI as evidence of the failure of security measures. Similarly, while some participants expressed faith in future control mechanisms, others doubted whether control would ever really reside with consumers in any complete sense. These different assumptions continued to resonate throughout the discussions.

Your credit report is electronic, you know. All these different things are kept for you. So if you think about it, those are protected, and this can work too.

b. Access to personal health information outside the health care continuum

The facilitator posed a series of questions about possible uses of PHI outside the health care continuum: research, public health, insurance, employment and marketing. A wide range of views surfaced on these complex and interrelated topics. The participants understood the concepts of de-identified and aggregated data applying the analogy to the use of Census data.

The great problem with a transmittable electronic medical record is I see that slippery slope starting, and I don't see an end to it once it can be easily accessible. I see social workers saying, well, we ought to be able to look at it, too, because we are acting in the best interests of the children. If it's in an electronic form that can be easily transmitted across the country, the slope becomes very slick, and I think I would certainly like to know who has accessed my medical record.

Most people favored "public good" uses of de-identified and aggregated PHI data for research and public health surveillance. Their privacy concerns closely tie to worries about losing health care coverage and jobs. Most are averse to sales-oriented marketing using their PHI. They want stringent protections against, and strong punishments for, abuses of their identified PHI if used to deny them health insurance coverage, discriminate against them in the workplace, or try to sell them products and services.

I'm for always giving people the option of opting out of things that people should have control over. But on the other hand, the way I see this particular thing is, this is one of the perks of having a nationwide system for data gathering of this sort. And as long as there are no names and there is no identification, I would want it available because I think it is a tremendous resource — a perk that comes out of something else like this. For all the different diseases, if they could access information with a database like that—I mean statistics—it would be fantastic.

Several general themes arose that cut across the sectors and uses. First, there was at least one voice in each group for broad access to aggregated, de-identified clinical data in the interest of stimulating innovation. One person described aggregated data as a public good and speculated that mining this resource for research and other applications could yield public benefits. Another believed that the responsibility belongs to policy-makers in determining the appropriate uses of PHI for the public good. Some participants doubted if those responsible for de-identifying and aggregating data could be trusted not to re-identify individuals or allow others to do so. Other fears were of hackers gaining access to the data, re-identify individuals, and doing harm with the information.

I sort of look at it as part of what we could do for the public weal. It can be used for all kinds of stuff. This strikes me, once it is de-identified, as being more like Census data, and we as a people, as a government, ought to be able to use it that way.

Depending on the context and purpose for non-clinical use of their health information, the participants varied about approaches to individual and systemic control.

1. Research

Many participants knew of the potential research benefits of access to de-identified electronic clinical data, including less expensive research leading to possible new cures. Those

living with serious health conditions were particularly aware of the importance of research and the benefits of using clinical records for this purpose. Several were already involved in clinical trials, and many were familiar with clinical and epidemiological studies of their illnesses. Still, some members did not want their PHI used for research, even in de-identified and aggregated forms. Many wanted to be able to choose to grant access to their PHI, the opt-in method.

I don't have a problem with [research use of my de-identified PHI], if it's going to help somebody else. At least I know my name is not going to be on it, and maybe the things that are going on with me, the medications or whatever, can help them find something better for the next person. I don't see how anybody can have a problem with trying to help better the medicine field. I would love to give back something to help another person coming behind me. See, I came in this world with nothing and, to get a cure for this [HIV], I would leave with something.

The question of profit complicated the topic of research uses of PHI, both identified and de-identified. Many participants drew a distinction between profit-oriented research (pharmaceutical) and government-supported, academic research. Some want paid when financial benefits occur, while others commented that contributing to research of any kind was enough of a reward. Several people want to be asked for permission to use their de-identified PHI for profit-oriented research but not for academic research.

The practice of recruiting subjects for clinical trials was given as a possible use of identified electronic PHI with potential "public good" benefits. Most participants agreed that for this use people should be able to opt-in.

2. Public health

In a public health setting, like if I had some infectious disease—say tuberculosis—somebody should be able to have access to it. But the information should be available only to them and only for that purpose.

Nearly all participants agreed on the importance of government access to their de-identified PHI for specific public health purposes. Several described public health uses of clinical information as one of the great benefits of an electronic system. Some noted that PHI is already reported and put to public health uses—a practice that one called "a long, honorable tradition." In contrast, one participant

asserted that he owed society nothing and would derive no benefit from things done for "the public weal."

I actually think, at least in some of these situations, that not only should we want some responsible government agency to have the information, but I think it should be mandatory. I think you shouldn't have the chance to opt out. It has a long honorable tradition, going back to the Plague. We live in a more and more mobile society, and it is more and more important. I know not everybody trusts the Government, but we have to trust our Government to look at and decide what the problem is and at least notify us that maybe we've got a problem.

Several people described public health's use of electronic PHI as a "slippery slope." Access to such information was a new form of governmental power. People fear that when government obtains easily transportable PHI for public health purposes, it will use it or let others use it for inappropriate or harmful purposes. They fear the government using personal information to interfere with their private decisions and activities. A few people pointed to new forms of social control that EHRs could facilitate, such as forced immunizations or taking children away from their parents. One focus group also envisioned a hypothetical health-related abuse of data on small populated areas of environmental health hazards. Their scenario—a form of "redlining"—was that health insurers would discriminate against people from a neighborhood with dangerous concentrations of lead in the ground.

I think when government gets given a power, that power tends to expand unless otherwise checked. I don't trust the people who want the door opened to close the door.

Despite the wide variations in their trust of government and security mechanisms, most participants accept the notion that government must have access to de-identified health information for public health purposes. Most agreed that government should be able to restore individual identifiers to de-identified data to trace infectious disease and other public health risks. Their differing opinions related to the alternative basis for participation—opt-in, opt-out, or mandatory. Some people argued that Americans should have no choice over the public health uses of their PHI; others wanted to retain the right to opt-in or out of such a system. Some wanted to be notified of the public health uses of their data; others thought this was impractical. And some thought

that information use for public health purposes was inevitable, based on precedent and law, and that abuses should be deterred with stiff penalties.

3. Health insurance

Most of the discussion of health care insurance uses focused on access to identified PHI. All three focus groups talked at length about the participants' sense of vulnerability, knowing they could lose insurance coverage and even health care treatment as a result of their health information. Several people described struggles with insurance companies including denied coverage for health reasons. A few people pointed out that genetic testing could exacerbate the risk by compounding what one called "the pre-existing condition label." The clear message from these consumers was that insurers' access to their PHI should be narrow and based strictly on the need to know with strong penalties in place for abuses. One person expressed trust in her personal physician controlling access as a way to protect PHI "from an insurance company or anyone who is malicious in wanting more information."

To take care of the other problems that I hear about insurance companies and employment and that stuff that I feel very strongly about, they shouldn't have access to this kind of information. That has to be taken care of by regulations and by giving -- perhaps creating new causes of action for that under specific statutes that make it very draconian, so people won't want to do it because it costs them money.

There are insurance companies, ladies and gentlemen, who are creating their own PHRs and EHRs, and also employers. That to me is very scary. As this information gets out there, my concern is that my right to health care insurance or coverage is going to be conflicted and that I am not going to have any. On the Internet, once you are out there, you are out there. You can't bring it back. So we have to be really [clear] in our policy, really clear about what that information is going to do.

Although they recognized that health care insurance companies use identified PHI for payment purposes, the participants showed different levels of awareness about the extent of insurers' legitimate access to PHI at present. Some remarked that they didn't want their insurers to see their health records, while others responded that their insurers needed, and probably already had, access to at least some of their information in order to make payment decisions. Adding another perspective, one person commented that the enrollees in public programs such as Medicaid and Social Security Disability Insurance (SSDI) may feel they have

already signed away their privacy rights to qualify for these programs.

In contrast, some participants questioned whether electronic records would make people any more vulnerable than they are in a paper system. They argued that insurance coverage is already tenuous, and a conversion to electronic records may have little negative impact. A few people suggested that EHRs could enable new privacy protections that are not possible with paper records, such as by allowing access to limited PHI rather than an entire chart.

In general, the health care insurance topic drew every focus group into animated discussions of broad health care financing and coverage issues. Several participants called for fundamental change in this area and even asserted that universal health care should be in place before EHRs made people more vulnerable to losing coverage. One person focused on the mixed nature of the insurance business. He called for a clear separation between health care insurance and other insurance practices, asserting that health care insurance companies should be required to divest of their other insurance interests. One focus group touched on the grey area occupied by Health Maintenance Organizations (HMOs), which provide both health care services and payment. This conflict of interest was pointed out by one participant enrolled in an HMO while also citing its strong prevention practices which benefit both patients and the bottom line.

4. Employers

Because most private health care insurance is obtained through employers, the worries about employers and PHI

paralleled those about health care insurance. Many participants expressed strong concerns about their employers having access to their PHI and discriminating against them as a result. Health information employers should be able to access must only relate to the employee's ability to perform a given job. People recognized that some employers are self-insured, blurring the line between insurers and employers. They stressed the need for strong firewalls between the insurance and other activities of self-insured organizations. The need for regulations and strong penalties was reiterated in this context. One person noted that the Americans with Disabilities Act already places some limits on what information employers can see.

A lot of large companies are self-insured up to certain levels. So you have a real problem of how to keep this away from your employer. And then, of course, the hiring decision. It's a big problem, and I think this is a good time to address it.

5. Marketing

The term "marketing" refers to a broad umbrella covering market research as well as direct marketing for both commercial and public-interested purposes (social marketing). The discussions focused primarily on commercial marketing.

Most participants did not want their PHI used for commercial marketing purposes without their express permission. One participant described experiencing abuse by having unwittingly been the target of direct marketing after using his credit card tracked his interests through purchases. Some people described being directly marketed for products or services related to their health conditions. For example, one was contacted by a care management company during her pregnancy—the contact made her "feel creepy." She would prefer in such instances that her physician control the contact based on whether she is benefited by the service.

I remember getting a [credit] card. A year later, I remember getting everything about CDs, everything about photography, everything about jazz. I didn't contact any of those companies, [the credit card company] did: "This is what he buys."

A range of opinions surfaced about controlling their PHI for marketing purposes. One person felt that aggregated, de-identified data should be widely available. Most members, when asked if people should be allowed to sell their own PHI, said that even if it were harmful, people should be able to sell it.

3. Operationalizing Control and Safeguards

To launch the discussion about operationalizing control, the facilitator described different levels of information security, including those used in banking and by the Department of Defense. By polling each group, he confirmed that the participants want a very high level of security for their PHI. Most want the level used for Department of Defense information, or higher. A few said the level used in banking was high enough for them.

Whichever system implements this needs to do their homework, and do it really well. I want computer scientists to look at all the code that is going to be used in the system and give me their expert opinion as to whether or not this is something that's secure. I don't want somebody coming out and just saying "Oh, it's using encryption, it is good."

The participants varied in ideas for how best to achieve security. In considering alternative safeguards and forms of control, the participants explored both the options available to individuals and the systemic controls possible through laws, regulations and penalties. Their views also varied as to the proper balance between individualized and systemic approaches. Those who favored an emphasis on systemic approaches (laws, regulations and penalties) used several arguments: the cost and complexity of individualized controls, the need for information in health care, the adequacy of safeguards, and the infeasibility of total individual control. Those making the case for individualized, case-by-case controls expressed little confidence in the

The reality is that time is being rationed with those physicians in a big way. So that we also have to think just about the practicality of how we set up the communication and how at certain points we can review the decisions we have made in relation to access and non-access.

systemic prevention of abuse in a consolidated information system.

People suggested building on existing public policies—for example, those on consent, mandatory reporting and emergency protocols—to avoid "reinventing the wheel." An exception was waivers, which generated considerable discussion in one group. One member felt that narrow approach to waivers (or permission) would be necessary because electronic systems combined with genetic testing will make people more vulnerable to harm through their PHI. In contrast, another—focusing on convenience—said she would be happy to sign a single waiver once and for all instead of every time she goes to the doctor.

Looking at safeguards from a broader perspective, one participant stressed the need for vigilance by institutions such as the news press and the American Civil Liberties Union (ACLU). He spoke of the importance of "watching the watchers" to ensure that they act quickly and appropriately with PHI at their disposal.

I am not sure I trust the powers of the watchers to act quickly on the basis of the information provided. My confidence in that diminished immensely after Hurricane Katrina. As the powers that be watch us, we should have more power to watch them; and as one increases, the other should increase. I would hope that the ACLU or something like that would be diligent and watching, and the press would be careful to report errors, and things like that.

In the future when we all have our own genetic code information, somebody can say, "I want a waiver. I want you to sign a waiver that says we have access to your entire genetic code, so we know every genetic predisposition you have." You have to deal with the waiver issues, because the real world is that all these entities are going to want to do things that will essentially negate everything we are talking about.

a. Opt-in or Opt-out

The diversity of the participants and the number of topics to be covered made it difficult to determine whether everyone fully understood the terms "opt-in" and "opt-out" as control options. However, all three groups expressed an explicit preference for the ability to opt-in to having their PHI in electronic form. This concept was articulated in one focus group by a member who called it an "active choice" by the consumer to participate in an electronic system. Another

I think it is probably more important to regulate, so if you are a good person doing good things, you have no fear of it; if you are looking for profit, you should have a major problem.

I think what we are hearing here is that ideally this thing should start out and hopefully stay as an opt-in program—patient opt-in, meaning that the technology is there and the patient has to make an active choice to have his/her files be accessible.

person observed that simply having this choice would increase the public's trust in the use of HIT and EHRs.

This is an issue that raises privacy concerns of people who object to the electronic system, that if you put out something like this, you do kind of have that sense of "Big Brother is watching you" and tracking where you are going, where you have been. So I think you would get more buy-in into this kind of system if people were given the option of being able to say, "No, I don't want to participate" — unless it is legally required already.

Two others contended that an opt-out system would create a stronger social safety net because people would be included unless they actively chose not to be. These participants reasoned that disabled or underserved people who did not understand the opt-in decision and were not properly instructed by their providers would be better off within an electronic system. One person took that logic a step further and recommended default deadlines so that people who don't "show up at the gate" automatically opt-in.

There is no one-size-fits-all for this solution, especially when you are talking about low literacy, low health literacy. An opt-out system would be better because you want to make sure there is a safety net for everybody. Because some people just might automatically not opt in, or providers will fail to offer the option, or they might not understand you have to opt in.

Some people expressed concern about the social and personal consequences of non-participation in the electronic health information system, whether it was through opting out or refusing to opt-in. One person said, "You can't just foul up the system by saying, 'I'm not going to play.'" Another wondered if she would have to pay higher insurance rates because her physicians were paying for more expensive malpractice insurance. Others worried about compromised public health statistics and worsening population health if too many Americans failed to participate. Based on concerns such as these, one group member felt that the Americans who choose not to participate in an electronic health information system should have to bear "a heavy burden."

Are we going to allow people to opt out of the whole thing, to be able to live in their bunker in Colorado and just not be in the system? I think the policy comes out on the side of this: If people don't want to be involved in any kind of insurance program, I guess they will be able to do that, we won't make them [participate in an electronic system]; but if they want to be involved in any kind of insurance program, they are going to have to do this. So it's their choice, but there really is a heavy burden to not doing it.

b. One-time consents for specific uses

The participants recognized one-time consents as an option that lies midway between wholesale blocking of information

and blanket permission for access. They could envision a number of contexts and uses of their PHI for which they wanted to be asked every time the information was requested. Examples include research uses by profit-making companies; clinical trial subject recruitment; product and services marketing; and access to particularly sensitive health information. In such cases, their permission for access would depend on the reason the information is needed.

c. Audit trails and notifications

All the participants expressed a strong desire to know who had seen their PHI both at and beyond the point of care. When asked about it explicitly, one group nodded their heads in emphatic agreement when a member declared that knowing "who has been there" is "the main defense against everything else." He quoted a fitting maxim on the subject: "Conscience is the small voice that tells you someone might be watching."

This is your main defense against everything else—to be able to tell who has been there. It casts light where there is none. That is the beginning point for solving any other kind of problem. To me, that is enormously important.

All the focus groups discussed various ways people could be informed of the uses of their PHI. While only one group expressly used the term "audit trail", they all discussed this option in functional terms. Some participants believe a greater advantage for tracking who accesses their PHI will be through an electronic system over paper forms.

Private detectives have made arrangements with people in the public sector to sell information to them. So somewhere we need to draw a line and make it really hard — not only hard to do, but dangerous to do. You know, we lost a Vice Presidential candidate because of his mental health records. There needs to be a really clear delineation, and that isn't there now.

Direct notification is another way these consumers can know about access to their PHI after the fact. While some people were satisfied with being able to review audit trails, others said they wanted email notification of every instance of access. A third option, preferred by some participants, was to

be notified only of attempts at unauthorized access, as happens with anti-virus software.

Dr. Rippen raised a scenario that illustrated an occasion when people felt notification was in order: PHI that a consumer has blocked is revealed to the physician through a flag in a laboratory or pharmacy information system. People responded that they would want to be notified that the information had been revealed to the doctor.

d. Laws, regulations and penalties

Many participants pointed out the limits of individual control mechanisms, the potential for serious abuse of PHI, and the need to augment individualized controls with an additional layer of security. They want policies, regulations and laws to govern use, with stiff penalties for the disclosure and abuse of information and for discriminatory practices based on health information. One group applauded when a member used the phrase: "…with serious punitive damages for unauthorized use." Another spoke of regulations as a way to block access for those "looking for profit." One participant cited the fate of IRS officers who reveal confidential tax information as an example; another mentioned accountants who misuse clients' information.

I think it is probably more important to regulate, so if you are a good person doing good thing, you have no fear of it; if you are looking for profit, you should have a major problem.

This is why it is important for individuals to be aware of these dangers, for people to be politically active in terms of trying to get laws passed to safeguard the information. You really can't control it past a certain level of certainty. You can try to, but you definitely have to make sure that you have laws on the books that guarantee serious punitive damages for unauthorized use of the information.

Many people described these systemic measures as a way to create a more functional and secure health information system, given the limits of personal controls. Several participants spoke of the key role of consumers in influencing public policy and lobbying for legislation to protect health information.

4. Consumer Rights and Responsibilities in an Electronic Age

Two important areas discussed about the conditions for successful and effective use of electronic PHI included what consumers should do for themselves, and what government, health care providers and other facilitators should do for consumers. This section addresses consumer responsibility.

The ability to view and correct their records is one reason many participants are receptive to EHRs and EHR systems. When asked about consumer responsibility in an electronic age, participants focused on the need to regularly check the accuracy of their records and inform their providers of any errors similarly to checking one's credit report.

It sounds like the credit report kind of deal where you get your credit report and realize all of the mistakes, and you have to deal with all of the credit bureaus. After a doctor's visit and they wrote something that you didn't agree with, you could even just have like a little simple check box that would just simply say "disagreed with" and then limit it by characters on why.

It seems like the only way this type of system would work is like the doctor-patient relationship on the electronic level where the confidentiality remains between the patient and the doctor about all of this information, and it's still primarily the doctor and patient, and they have to protect that relationship and protect this information.

The discussions highlighted the challenge of striking the right balance between self-reliance and reliance on a trusting doctor-patient relationship. One person spoke of doctor-patient confidentiality as the cornerstone of a viable electronic system. Another predicted that EHRs would forever change the landscape of that relationship by turning patients into partners in their own health management. She asserted that government should strengthen consumer empowerment by encouraging consumers to be more engaged in their health. Some participants warned of the time pressures on doctors and the practical constraints on doctor-patient communication, and others called for realism about what consumers can do for themselves.

I do feel like there is a certain integrity in the medical field, and that a lot of the talk and what is going on almost seems to change that. It is very bothersome to me.

I think it is so important that we empower ourselves, that we be our own advocate. We have to.

Participants' views about consumer empowerment and their ability to partner with other stakeholders hinged on their

sense of the public's capacities to exercise responsibility and make appropriate decisions. There were enthusiastic voices for empowerment—notably from the individuals involved in consumer self-help and advocacy activities and some participants were more skeptical. A more common view was that Americans differ in abilities to form partnerships for health management because of their diverse cultures, levels of education, income and technology access.

One person articulated a bottom line: consumers will be responsible for understanding the implications of their choices when controlling their PHI, and must be willing to take the consequences.

I think what this HIT movement will do is really validate us as partners with our medical providers—and not just as being receiving care, but actually participating. I think that patients should be open and frank and up front with their doctors. But there may be situations—rarely—where information doesn't want to be shared, and that patient has the right. They are doing it now by not talking about it.

This morning we were talking about stupid people that can't make proper decisions, and now we are acting like they have a medical degree. I mean, there are doctors for a reason!

5. Systems and Supports Needed for the Consumer to be Informed

As to what and how government, health care providers and others could help consumers become better informed in exercising their right to control access to PHI, the participants had several suggestions. Their comments addressed both their personal concerns and awareness of the needs of other consumers, including underserved segments of the population.

I think one of the roles of Government—maybe public health—should be to get the word out that people need to be more engaged. That they should encourage us as health consumers to be more proactive in our health care. As an advocate, one of the most important things that I do when I talk to families is to say it's okay to ask for a second opinion, it's okay to ask for the record. And all I am doing is giving them permission. I would like to see a more proactive approach on the part of the Government in helping consumers do that.

People in all three groups raised concerns about the digital divide and health literacy. One person referred to the "opt-out" concept to illustrate the digital divide. Just as some New Orleans residents did not evacuate before Hurricane Katrina because they had no cars, people without technology "are not opting out by choice, but because they have no way to get in." Another participant spoke to the issue of persons with cognitive disabilities. She pointed out that the many Americans with mental illness—some of whom face economic disadvantages, even homelessness—will need extra support to benefit from HIT and to exercise their right of controlling their PHI.

If we are trying to establish one equal system that everyone has to follow, then, you will have to provide opportunity so that everyone can access that information.

When asked what conditions would contribute to the success of an electronic system, the participants proposed ways to extend the opportunities and benefits as widely as possible. One recommended a well-crafted marketing effort to promote HIT to the public. Several stressed the need for hands-on help in educational programs as well as clearly and appropriately targeted written materials e.g. literacy. Some

I think it's a good idea for consumers to have control. My only problem is with the language they use. Most physicians talk to you like you are a physician, and you're trying to figure, well, what the devil is this?! But I still think it's a good idea.

suggested using community networks to widen technology access via churches, high school health classes, public kiosks, and terminals in doctors' offices.

I just worry that we are going to make it so very complicated. Paying taxes should be pretty easy, and we all have to hire CPAs. And once all the different interest groups get involved with what they want out of this, we may need to hire health negotiators, and that would be a shame. We just need to keep it simple.

Other practical suggestions included:

- make paper print-outs of EHRs available to people with limited technology access.;
- keep control mechanisms simple.;
- give health care providers a role in explaining EHRs, information uses and control options to their patients;
- provide answers to questions such as these:
  - what are my choices and what are the implications?
  - how do I correct my record?
  - what de-identified information will be shared, and for what purpose?

Simplifying the information that people need to know, so that they can understand. Like if it comes out like "Do you want your genetic information available?" people have to know what that means, the implications—like medical knowledge awareness. I wonder if this could even work unless you almost put people through a kind of thing like we're going through, like a training. Issues to think about. I wonder if it is really going to be enough to just send somebody a flyer and say, this is what is coming down the pike. I mean, look at all the stuff we've had to think about and rethink! My question, I guess, is, is it going to be practical to work this? Too many choices become overwhelming and paralyze people.

The participants also suggested the following tools and functionalities to help consumers make informed decisions:

- a medical encyclopedia;
- report cards on caregivers;
- information on clinical trials;
- information on the standards of care;
- periodic reminders to update one's information.

Significantly, several people remarked on how much they had learned in the course of this focus group process. One remarked that consumers will need "training" to be able to fully benefit from electronic health information systems and exercise control effectively. He cited the focus group discussions themselves—"a kind of thing like we're going

through"—as a model. Another spoke of the merits of public debate to allow consumers to speak, listen and learn.

6. Broad-brush Summaries

Toward the end of the discussions, Dr. Bartlett asked the participants to summarize their best hopes and worst fears in relation to electronic PHI. The following compilation lists the elements mentioned in each category.

I think an upside would be we have more efficient and more effective ways by which consumers have access to the information, which in turn would relieve a treasury someplace of a fiscal burden. The downside can be if it were to get in the hands of insurance companies.

Best hopes

- portability with an easier time changing doctors;
- PHI available in order to take care of me and my family;
- all my doctors seeing all my information and acting as a team;
- better emergency care;
- ability to make better health decisions;
- people getting treatment whenever and wherever they need it;
- being able to provide doctors with complementary information;
- having a permanent record to help me stay healthy all my life;
- access to supplementary information on health and illness;
- freedom to opt-out;.
- less expensive care;
- doctors having more time for their patients;
- better preventive care;
- nationwide health care;
- better management of my records as I get sicker;

Another part of it for me is having all of my physicians be a team, that they are able to access the other, because it -- in a lot of cases, they need to know what has been happening elsewhere in my personal medical history, and I am sure it is true for other people. I think that, again, in addition to my being able to access everything, having them be able to do all of that, and also being able to add things. The downside, what scares me is the idea of having a multi-region or national system where there is information on me out there that I don't even have access to, but any provider anywhere, even if they are mine or not, would have access to that information.

- ability to address public health issues resulting in a healthier population.

Worst fears

- inability to get insurance, loss of health care;
- employment discrimination;
- a system in chaos, destruction of the current system;
- digital divide thus widening disparities;
- hackers;
- privacy invasions;
- the wrong people getting the PHI and using it to people's detriment;
- false information inputted by third parties;
- government agents kicking down doors;
- profiteering;
- redlining;
- multi-regional or nationwide system where others have access to my PHI without me having access to my own PHI.

My fantasy is to have a nationally portable uniform system with uniform inputs, so that I could access and any provider I care to go to could access instantaneously, more or less, this data, so that my friends, executors, whoever controls my powers of attorney, whatever, the people who need access could have instant access to that, that emergency people have instant access to it, that researchers can use for these nice long longitudinal studies that are so expensive to do these days -- because I think that is part of what we can all give back. It doesn't even hurt. The nightmare is that it will form as a whole series of non-interoperable systems that are proprietary in some way or another, that there will be large information leaks through great big gray areas, so you won't really know where this stuff is going or what has really happened to it, and that would be very unfortunate.

7. Consumer As Citizen

Through the course of the day, participants increasingly approached topics from a societal perspective as well through the lens of their personal interests. There were several references to the role of law and public policy. Some voiced serious doubts about the trustworthiness or competency of government. Others spoke of the central role of government in developing a workable information system, determining access to PHI, implementing protections and punishing abuses.

If you have an electronic healthcare system, and the only response is "Trust us, this is for your own good, and that cod liver oil is mighty tasty," that isn't going to work. You have to have transparency, at least to experts, and you have to have punishments that work.

First of all, I want to thank you for this. I love giving my opinion, and the idea that you pay me to give my opinion is great, and it's been a real honor be with you all.

Recognizing the importance of public policy, many expressed enthusiastic appreciation for the chance to give input through these focus groups. Several expressed interest in the Department's reasons for conducting these focus groups and its plans for using the findings. A number commented on how much they had learned in the course of the discussion, noting the ways in which their thinking had changed. As a result of the discussions, some said they had become more cautious and less "naïve." At the same time, others who had been negative about EHRs were willing to join in the discussion of how to optimize the new health information system, which many regard as inevitable.

I think it will be very useful, maybe even critical, to have like standing groups to advise HHS — ongoing consumer groups, lawyers and so on—to be able to bring these things as they change, new things, new issues, think it through in an ongoing group. I mean, this is great, this focus group; but I am sure if we thought about this and had more information as things change, we might have different perspectives. Make sure there is like a sustained formal input mechanism and that they implement this very gradually, but not until all of these issues are really worked out.

Several people asserted that consumer participation in discussions such as the focus groups add great value, not only as a mechanism for public learning but also to generate good public policy. One person suggested that consumers be engaged in "a sustained, formal input mechanism" to advise DHHS on developing the nationwide health information network. Others stressed that the partnerships between consumers and other stakeholders to develop this network must begin immediately, at the planning stage. There was a strong feeling that *the time is now* for consumer participation in public policy development and that public debate and involvement are essential to arriving at appropriate solutions.

I think public debate is necessary. Without public debate, the decisions are going to be made that you have no idea about. But also, public debate will allow anybody who wants to partake in the debate to get involved. And you can learn things, look at things from a perspective that you haven't even thought about as well as have your opinion swayed or sway other opinions, versus people looking through it with blinders on about their own personal situations that may not be applicable to one of us in the room or the other 290 million people that we have walking around this country. So I think the debate is a positive thing—not to do things in secret.

One focus group explored their views on the role of consumers with respect to the relative benefits and risks of electronic PHI. Early on, a member had commented on the "hazy" benefits of health information technology; another remarked later that its risks were being underplayed. Picking up on these comments, the facilitator asked the group to weigh in: Were the risks of electronic health information

A lot of people can imagine lots of benefits. I think we talk about the negative because people putting the system in, they get caught up in the benefits and they get excited, and they just stop thinking about how it can go wrong. Most people can think of plenty of benefits. It's the misuse that concerns us.

being underplayed and the benefits overplayed? In response, people said that while they could think of many potential benefits, they saw their main contribution, as consumers, in pointing out the risks. They spoke of the need to temper the zeal of the experts about the potential benefits of new technology—"They will make sure they tell you the benefits"—with the potential risks.

I think the benefits will be there, but that they are being overplayed. Because in any system, they will make sure they tell you the benefits. So now it is our turn to figure out what's wrong, and that's why here and now, people are talking about the things that we see wrong.

A clear messages to emerge from the discussions was the critical importance of *transparency* to consumers. The participants want to know how electronic systems and networks work, in detail; they do not want secrets or surprises. One member summed it up for the group: "Just keep us informed. Tell us the good, the bad, and the ugly." The message of transparency thus stands alongside those of responsibility and participation in defining the conditions for effective consumer control.

Will we really have the choice? —I think we do. I think now is the time. Technology is taking off, and the policy and laws haven't moved up. So now I think -- being an optimist -- this is our chance to really make a statement as consumers and in a public venue that this is what is happening, this is what is coming down, and we want a voice, we have a seat at the table. You're right. A lot of this stuff is being collected and handled, and it sounds scary, but I guess that's why all of the information has to be on the table, so that we know, so that we can say at the policy level and then the legislative level, this is what we're willing to live with as consumers. We want to maintain a consumer focus.

APPENDIX A. Consumer Focus Group Questions

1. Overall reaction to the introduction/context (response to the presentation)
    a. General comments
    b. What do you expect this can do for you? Hopes
    c. What are your concerns? Fears
2. Control

"Consumers have control over their electronic health record"

    a. What does it mean?
    b. Is it important and if so why (if not, why not)?
    c. Do you control health information now?
        i. If yes, how? Is it adequate? If no, why not.
        ii. How would you like to control it?
    d. How would you like to control health information in a healthcare system that is electronically connected? Do you think it is different? If yes, why?
3. Control often covers a lot of topics from who is allowed access, what information is available to them, who can change this (why and when).
    a. Do you want to be able to control access to your health information?
        i. If yes:
            1. Who should be allowed to see your health information?
            2. Why should they be allowed to access your health information?
            3. When should they be given this access?
            4. What part of your health information should they be able to access? [Should you have the ability to control what parts of your health information can be seen by different people?]
        ii. If not:
            1. Who should be allowed to control access?
            2. Do you want to be told when someone accesses your health information? If so, how should that be done?
4. In-depth discussion on control
    a. Who do you want to let access to and under what conditions?
        i. Should you always be allowed access to all of your health information? What shouldn't you need to see?
        ii. What information should be made available in an emergency?
        iii. How should permission be granted?
        iv. Should permission to use your information be asked for research? Public health? Why or why not.
        v. Should family members and non-clinical caregivers get permission? How should that permission be granted if you are not able to (unconscious). Why?
        vi. How should permission to access you health record be provided to clinicians? Should it be your entire record or parts of it? Why?

vii. Should permission be requested for Health insurance companies requesting information? Should it be allowed access to your entire record? Why or why not?
viii. Should permission be requested for Third parties requesting information? Should it be allowed access to your entire record? Why or why not?

b. Should there be a difference in control for different types of information?
   i. Is information entered by the clinician or created for treatment different (as it relates to control) that something you enter yourself (e.g., personally entered data/diary)? Why or why not. What about labs or medications
   ii. Controlling based on category:
      1. Disease specific. Is different type of information more sensitive than others (e.g., HIV, depression, high blood pressure, prostate cancer)? If so, what makes it different? Would the capability of controlling access to your information by disease (e.g., HIV, depression, high blood pressure, prostate cancer) be helpful? Why or why not.
      2. Clinician specific. Does it matter that information is categorized by who the clinician was? Why or why not? If yes, would the capability to control access to your health information at the clinician level be helpful? Why or why not?
      3. Is there another category that may be useful to control access? Explain.
      4. If you could only control information in one way (disease versus clinician versus other) which would be the most useful? Why or why not?
   iii. Controlling access based on "level"
      1. Should different users of the system have access to different levels of access? E.g., should the receptionist see only you contact information and health insurance information or more? Why or why not?
   iv. Control once health information out of healthcare system
      1. What about information that is given to other entities, e.g., life insurers, employers, researchers? If access is allowed, is control ceded? Is control lost for a limited time?
   v. Deidentified versus identified
      1. What does identified or deidentified mean to you?
         a. Identified means that the information is shared with identifying information (e.g., your name, address) associated with it.
         b. Deidentified means that you can not be identified by the information.
      2. Would you like control over access to your deidentified information? Why or why not? How important is this?
      3. Would you like control over access to your identifiable information? Why or why not? How important is this?

c. Options for access
    i. What should be the settings for control (Opt-in or opt-out)? For example, should access to everything be allowed (for clinicians, researchers, and public health)? Why or why not?
    ii. Default settings. Should there be a default settings that can be selected? For example, default setting for general sharing, moderate sharing, limited sharing?
    iii. Minimum data sets. For uses of health information outside direct patient care, should minimum data sets be defined? For example, life insurance access to limited data relevant to setting premiums or eligibility.
d. Rights and responsibilities
    i. Auditing. How important is it to see who has accessed your health information? Why or why not?
    ii. Security. What level of protection is needed? More than online banking? More than pins? What industry should be the leader? Is defense too high?
    iii. Ability to modify access at levels (what levels). How do you envision changing access levels? How important is this? (disease, provider level, user type/person)
    iv. Consumer responsibility as it relates to control What are your responsibilities? If a healthcare provider can not access critical information, who is at fault for a bad outcome?
    v. Ability to make an informed decision
        What information do you need to make an informed decision about limiting access to your health information?

Appendix B. Background articles sent to the participants prior to focus group meetings

Health Records Of Evacuees Go Online:
Government Wants Doctors in Shelters to Have Data

By Jonathan Krim
Washington Post Staff Writer
http://www.washingtonpost.com/wp-dyn/content/article/2005091302128.html

Wednesday, September 14, 2005; Page A24

The federal government is making medical information on Hurricane Katrina evacuees available online to doctors, the first time private records from various pharmacies and other health care providers have been compiled into centralized databases.

The data contain records from 150 Zip codes in areas hit by Katrina. Starting yesterday, doctors in eight shelters for evacuees could go to the Internet to search prescription drug records on more than 800,000 people from the storm-racked region.

Hurricane Katrina brought unprecedented destruction to the Gulf Coast. View the Post's multimedia coverage of the disaster. (Reuters)

Officials hope to soon add computerized records from Medicaid in Mississippi and Louisiana, Department of Veterans Affairs health facilities, laboratories and benefits managers.

The records are one step in reconstructing medical files on more than 1 million people disconnected from their regular doctors and drug stores. Officials fear that many medical records in the region, especially those that were not computerized, were lost to the storm and its aftermath.

Although the immediate focus is on urgent care for hurricane victims, participants in the effort say the disaster demonstrates a broader need to computerize individual health records nationwide and make them available throughout the medical system. Such a step could, for example, give emergency room doctors a way to quickly view medical histories for late-night accident victims.

Electronic health records are controversial among many privacy advocates, who fear the data could be exploited by hackers, companies or the government.

Ray Fowler, head of medical relief operations in Dallas, said "it was extremely scary" for doctors to have no records to rely on as thousands of evacuees poured off buses with serious injuries or infections.

Some patients had been on various medications before the hurricane, for conditions such as high blood pressure, but did not know what prescriptions they took, Fowler said.

Currently, roughly 8,000 people are in critical care shelters, while other seriously ill patients are being treated in hospitals outside the Gulf Coast region. But many of the 250,000 evacuees in various shelters also need medical attention.

"We think this could help save some lives," said Dr. David J. Brailer, coordinator of health information technology for the Department of Health and Human Services, who is spearheading the effort.

The system took about 10 days to organize, with daily conference calls involving as many as 60 state and federal officials; emergency medical providers; insurance, pharmacy and medical-software company representatives; and government lawyers.

Participating pharmacies so far include CVS, Rite Aid, Albertsons, Walgreens and Wal-Mart. Expected to be added soon are Winn-Dixie, Kmart and Target.

Brailer said he was concerned throughout the process with privacy issues. Only medical personnel at the various shelters and hospitals treating evacuees will have access to the information.

Federal regulations do not require patient consent for their records to be shared for medical purposes. Companies or organizations that have such data must have formal agreements with each other before data can be exchanged, but the government said it would not enforce those rules while Katrina victims were in need, as long at the entities had verbal agreements to use the data for the relief effort.

States with more stringent regulations suspended their rules as well.

"We've been extremely cautious," Brailer said. "There were a lot of things we could have done that we didn't do."

Brailer said in his original vision, the database program would end once evacuees are permanently resettled, either back in their home communities or elsewhere.

Others involved in the effort, however, already are discussing ways to enhance the system and create personal health records for those who might need to move frequently over the next several months. As constructed, the databases do not allow doctors to update the records with information on treatment provided in the shelters.

"We're already preparing for a second wave of victims who have been in hotels but the money is running out," Fowler said.

The Bush administration and the pharmaceutical and technology industries have long argued that standardized, individual electronic health records that can be shared and quickly viewed would improve care and cut costs.

Electronic records also would speed the way for patients seeing different specialists, switching doctors or moving frequently in an increasingly mobile society. And they could be used to identify medical inefficiencies in the public-health system, proponents argue.

Even before the hurricane hit, Brailer's office was preparing to award contracts to create a "national architecture" for electronic records that every player in the medical system could use. The government is not mandating such a system nor will it operate it, Brailer said, but it wants to enable the private sector to do so.

On Monday, Health and Human Services Secretary Michael Leavitt named 16 people to a task force to advance the administration's goal of bringing electronic health records to most Americans within 10 years.

None is from a recognized privacy organization, and privacy advocates worry that even beneficial efforts during an emergency can expand beyond the scope of the original crisis.

Sue A. Blevins, founder of the Institute for Health Freedom, a medical-policy think tank, said she supports emergency programs such as the Katrina databases. But she said that "many things are done during a crisis that society normally would not accept."

Blevins opposes national electronic health records for individuals because the Bush Administration eliminated the right of patients to give consent before their health information could be shared under many circumstances.

"When you don't give people the freedom to decide how much information they want to share . . . the only choice they have is to either lie or withhold the information when they want their privacy," she said.

Medicine Slow to Modernize Recordkeeping

By LAURAN NEERGAARD
The Associated Press
http://www.washingtonpost.com/wp-dyn/content/article/2005/09/14/AR2005091400914.html

Wednesday, September 14, 2005; 11:01 AM

WASHINGTON -- Electronic medical records could improve patient care and possibly save billions of dollars, yet many doctors aren't investing in the technology because they may not reap the savings _ insurers and the government will, researchers report.

It's one of several pitfalls blamed for slowing adoption of computerized medicine in a collection of provocative, sometimes conflicting studies published Wednesday in the journal Health Affairs.

No more than a quarter of U.S. hospitals and 20 percent of physician offices have adopted electronic medical records, the RAND Corp. found. Usually, they're hospital- or doctor-specific, not easily transferred and read by other health care providers.

The ultimate goal of electronic medical records is a nationwide network, allowing quick access to, say, the medical history of a patient lying unconscious in an emergency room far from home. Other benefits could include paperless prescriptions to cut drug errors and software linking patient records to care guidelines and automatic checkup reminders.

RAND researchers set up a statistical model to predict the possible savings from such health care improvements and from improved business efficiency, such as eliminating redundant care and shortening hospital stays, if 90 percent of hospitals and doctors ultimately adopted such a network.

A conservative estimate came to $81 billion a year, $77 billion from improved efficiency and $4 billion from reduced medication errors and side effects, RAND lead researcher Richard Hillestad said.

Assume that patients and doctors actually follow checkup reminders and other software-spurred advice _ an unknown, Hillestad acknowledged _ and his model predicts savings could double.

Replacing paper records with such a connected electronic network would take about 15 years and cost hospitals about $98 billion and physicians about $17 billion, Hillestad estimated.

"The potential savings would not be realized immediately," and doctors and hospitals making the investments would get fewer of the profits, the study cautioned.

Instead, Medicare would receive about $23 billion of the potential savings each year, and private insurers about $31 billion a year, he concluded, saying those predictions justify more government funding of computerized medicine.

But another study from the University of California, San Francisco, found the technology not as expensive. Among 14 single or small-group physician practices, the average spent about $44,000 per full-time provider to establish an electronic medical records system and about $8,500 a year to maintain it, money recouped in business savings within 2 1/2 years.

Those were averages; some practices didn't recoup the investments for years. And the quality of the computerized systems varied, as two reported severe billing problems _ one nearly went bankrupt _ at least partly due to the system they adopted, the study found.

Most of the hoped-for improvements from electronic medical records are still hypothetical, cautioned Drs. David Himmelstein and Steffie Woolhandler of Harvard Medical School.

RAND's models in particular are based on "a disturbing array of unproven assumptions, wishful thinking," they wrote in a review of the research.

Moreover, nobody yet knows what computer features doctors should buy. A third study published Wednesday, from Boston's Brigham and Women's Hospital, said that in addition to record storage, systems should include electronic viewing of test results, paperless prescriptions, electronic claims submissions and secure patient e-mail.

But such systems will be useless unless the records can be shared between doctors and hospitals.

To help establish standards, Health and Human Services Secretary Mike Leavitt on Tuesday named a 16-member commission of representatives from hospital, doctor, insurance, government and patient-advocacy groups.

Emerging Technology: The patient-accessible EMR
By Gary Baldwin, for HealthLeaders News
Emerging Technology Series
http://www.healthleaders.com/news/print.php?contentid=72241

Sept. 19, 2005

When Pam Mullen needs to refill a prescription or view her latest test result, she heads promptly to her PC. Unlike most patients who use the phone for such chores, Mullen logs on to a secure Web site maintained by Group Health Cooperative, an 850-physician group practice based in Seattle. Within seconds, Mullen can access numerous services through a patient portal, "MyGroupHealth."

Because the portal is linked with Group Health's electronic medical record system, from Epic Systems Corp. in Madison, Wis., Mullen is free to navigate virtually the same medical record her physician sees-physician approval is needed before results or medical information is posted. If she has a question, Mullen leaves an electronic query for her doctor, and usually receives a physician response within two days. It's a major improvement over phone tag, she says, adding, "it doesn't take less time to get an answer, just less of my time."

Welcome to the world of the high-tech doctor-patient relationship. Their EMR installations behind them, growing numbers of hospitals and medical groups are taking the next logical-though controversial-step of granting their patients online access. Often combining chart access with other services, such as appointment and referral requests, such portals are gaining wide popularity among patients. Using sites like these, patients can access information that's otherwise difficult to obtain. Likewise, physician champions of online records access-dismissing fears of patient misuse-contend that the systems enhance the doctor-patient relationship.

But even ardent proponents of online medical records caution that for the technology to succeed, caregivers must first revisit their assumptions about informing patients. Providers may pay lip service to their patients' rights to see their own charts, whether paper or electronic. But in practice, many balk at the idea. "The industry mantra has been, 'No news is good news,'" argues Marie Savard, M.D., a Philadelphia-based solo internist and longtime advocate of sharing records with patients. "Every day someone's test results get put into a file and forgotten about."

Putting records online, however, keeps them front and center. Group Health's site, which launched a secure messaging service in 2000 followed by EMR access in 2003, generates some 26,000 unique visits each week among more than 87,000 registered users, says chief information officer Ernie Hood. "The service is convenient for our rural members who must drive a long way to see a physician," he says. But Group Health physicians-who are obliged to use the system-benefit too, adds Matt Handley, M.D., associate medical director, quality and informatics. "Physicians were worried about patients pestering them constantly," by overusing the online messaging function, Handley says. "But patients are very respectful of physicians' time."

Better patient relations

Granting patients online access to their own charts enhances the doctor-patient relationship, adds Daniel Sands, M.D., an internist at Boston's Beth Israel Deaconess Medical Center. Since the 556-staffed-bed Beth Israel began "PatientSite" five years ago, interest among patients and physicians-whose approval is needed before patients can view records online-has grown steadily, Sands says. Some 26,000 patients are registered users, up from 18,000 a year ago. About 250 physicians are participating. Through PatientSite, patients can see practically everything in their record, including lab results, radiology reports, med lists, allergies and culture results. Not visible are physician office notes and HIV test results. "Patients see exactly what the doctor sees," Sands says.

To make the record more intelligible, PatientSite often includes links to consumer-friendly explanations of procedures and tests. Likewise, Group Health physicians have hundreds of customizable, prewritten templates to draw from in responding to online questions from patients about their health or the contents of their charts. Triage nurses answer about half of the 7,000 weekly electronic queries, forwarding the rest to physicians.

Granting patients access to their charts paves the way for more productive office visits, says Group Health's Handley. For example, one patient with a shoulder problem reviewed both his record and some links explaining likely treatment options that Handley had dispatched through the secure messaging hookup. "He came right in, got on the exam table, and asked complicated questions about the risks and benefits of a cortisone injection," Handley recalls. "Instead of me having to explain shoulder mechanics, he knew what to expect from the visit."

Packaged with electronic communications options like secure messaging, online EMRs can be a strong lure to attracting patients, adds Cleveland-area resident John Quinn, a partner in the Health & Life Sciences practice at Accenture, a New York-based consulting company. Quinn should know. Last year he switched physicians to gain access to patient technologies offered by The Cleveland Clinic.

By offering online access to charts and enabling patients to pose questions electronically, practices may forgo office visit income. But many physicians say granting patients online access cuts down on unnecessary phone calls and boosts their practice's efficiency. "We push patients hard to use our electronic communications options," says Charles Kilo, M.D., CEO of GreenField Health, a five-member group practice in Portland, Ore., that grants chart access to patients via a secure Web site. To defray costs, GreenField charges an annual fee that ranges from $295 to $495, depending on the patient's age. Although 80 percent of GreenField's patients use the secure messaging and prescription refill functions, few want access to read their records. "The chart belongs to the patient, but most people don't want to see it," Kilo says.

In addition to serving patients, online record access can boost continuity of care with other providers, says Jim Skee, M.D., a practicing member and CEO of Silver Internal Medicine Inc., an eight-physician group in Silver City, N.M. The group practice started

a patient portal in 2004, granting patients access to almost everything in their chart except, for example, EKGs or progress notes.

The group also grants online access to home health and medical-equipment suppliers, says Tad van der Weele, system administrator.

For Kilo, granting patients access to their own records is the cornerstone of consumer-driven healthcare. It's a lesson lost on the industry, he contends. "Consumer-driven healthcare has been usurped by health savings accounts," he says. "The underlying sentiment is that if you make people have a financial stake, they will behave differently. But the optimal consumer-driven care is when people can be directly connected to the medical practice."