

Oregon Health Information Security and Privacy Collaborative (HISPC)

Oregon HISPC

Consumer Engagement Project

FINAL REPORT

October 2007

- Development and testing of consumer education tools
- Exploration of the consumer perspective on data privacy and security and issues of consumer access and control

Written by project consultants:

Jeanne McGee, PhD

Mark Evers, PhD

McGee & Evers Consulting, Inc.

1924 NW 111th Street

Vancouver, WA 98685

jmcgee@pacifier.com

mevers@pacifier.com

360 574-4744

Submitted to:

Jody Pettit, MD

Health Information Technology Coordinator

Office for Oregon Health Policy and Research

1225 Ferry Street SE

Salem, OR 97301

jody.pettit@state.or.us

503 706-2208

CONTENTS

EXECUTIVE SUMMARY	i
-------------------------	---

FINAL REPORT

PART 1: Overview of the Project.....	1
A need for consumer education tools.....	1
What did we do?.....	1
Who conducted this project?.....	2
PART 2: Developing the consumer education tools.....	2
Scenarios and topics.....	2
Development and revision.....	3
PART 3: Collecting feedback from consumers.....	4
Interview participants.....	4
Why did we use interviews instead of focus groups?	4
Interview methods.....	5
PART 4: Topic-by-topic findings with illustrative quotations.....	7
Strong consumer interest but limited knowledge and understanding.....	7
Reactions to the project's consumer education tools.....	10
Protecting privacy and security of the information.....	13
Views about who should see the health information.....	16
Controlling whether information is shared and who can see it.....	20
Conclusion.....	28
References	29

APPENDIX

A. Project team.....	30
B. Acknowledgments.....	31
C. "Secure Network" booklet	33
D. "Personal Electronic Health Record" information sheets.....	53
E. Profile of the consumers who were interviewed.....	60

EXECUTIVE SUMMARY

Most consumers have only limited awareness and knowledge of electronic health information exchange and what it means for them. To make fully-informed decisions in areas that affect them personally, they need specific and actionable information that is easy for them to understand and use.

Responding to this need for consumer education, the *Oregon Health Information Security and Privacy Collaborative* (Oregon HISPC) conducted a *Consumer Engagement Project* in late Spring 2007.

In this project, we developed and tested prototype consumer education tools and explored consumers' views about issues related to electronic health information exchange. The project team was the Office of Oregon Health Policy and Research; McGee & Evers Consulting, Inc.; Portland State University; and the Oregon Health Care Quality Corporation (*see Appendix A for details on the project team*). The project was funded by the Agency for Healthcare Research and Quality.

Written in plain language and illustrated with diagrams and examples, the consumer education tools we developed explain basic concepts and describe two different scenarios of electronic health information exchange:

- A 16-page booklet about *Secure Network*, a fictional data-sharing service for use by health professionals (see Appendix C). *Secure Network* is *not* intended to be a model of how data should be shared. Rather, we invented *Secure Network* and its specific features as a means to test basic explanatory language and as a device to trigger consumers' reactions to issues such as data privacy and security, opt out, and limitations on patient access. The booklet describes the types of health information that are shared and the safeguards for data privacy and security. In this scenario, unless patients take the initiative to opt out, information from their electronic medical records is automatically shared with any authorized health professional who requests it. The booklet tells patients how to block all or part of their information from being shared on *Secure Network*.
- A set of information sheets that outline key features of personal electronic health records (PEHRs) and contrast these features with those of *Secure Network* (see Appendix D).

To test these tools and explore consumers' reactions to the two scenarios they depict, we conducted 16 two-hour interviews with a demographically diverse group of consumers in the Portland metropolitan area and The Dalles.

Findings

The people we interviewed were very interested in electronic health information exchange in general and in both of the scenarios depicted in the consumer education tools (*Secure Network* and PEHRs). They saw value in making information from their medical records readily available when needed, especially during emergencies, when they travel, and when they see a new doctor. They saw value in the data sharing service designed for use by health professionals and they particularly liked the consumer access and control provided by a PEHR.

Interviews revealed many communication challenges including limitations in knowledge and poor understanding of basic concepts. The mechanics of electronic data storage-retrieval-transmission were very poorly understood. Limited knowledge also made it hard for people to put the topic of electronic health information exchange into a broader context. People knew very little about the multiple ways in which their health information is now being stored and routinely shared, sometimes with their knowledge and permission and sometimes not.

Overall, interviewees found the consumer education tools appealing and easy to understand. They found the detailed examples especially helpful and said the added length was not a problem. Interviewees made many positive comments about language, layout, illustrations, colors, and friendly tone. Many people emphasized the importance of the detailed examples. Although the booklet was 16 pages long, 14 of the 16 participants said the length was “just right.”

Data privacy and security were major concerns; people wanted to know about specific safeguards. People raised concerns about identity theft, unauthorized access, and possible misuse of their information. Recognizing that no system can be perfect, they were reassured by the safeguards described in the booklet. In particular, they liked that *Secure Network* (a) keeps track of who sees their information and makes a report of who has seen their information available to the patient; (b) requires users to be trained and sign confidentiality pledges; (c) tells them if security is breached and (d) punishes anyone who breaches security. Several people thought there should be oversight by an outside, independent organization.

Interviewees expressed great trust in health professionals and some distrust of others. Interviewees wanted their doctors to have easy access to their personal health information, and they were happy to see *Secure Network* described as being for use by health professionals only in the course of providing care. They responded positively to the list of specific exclusions that told how certain organizations such as health insurance companies were not

allowed to use *Secure Network* and that *Secure Network* could not be used to get patient information for use in fund raising or processing of payments.

People felt that patients had the right to see the information in their own medical records. The people we interviewed did not seem to perceive any barriers to patient access. They assumed that patients who wanted to see the information in their medical records could simply ask and their health providers would show it to them. Many of the people we interviewed had already obtained copies of their own records.

Many people thought it was okay that patients were not allowed to use the *Secure Network* to see the information in their medical records. For most people, giving doctors easy access was the main issue. Interviewees assumed that patients could use other means to see the information in their own medical records, such as asking their providers.

Overall, interviewees were quite positive about the consumer access and control offered by a PEHR, but they did have some concerns. They liked that having a PEHR was voluntary and that patients could add their own information to their PEHR and control who could see it. They had concerns about patients being allowed to make changes to their own medical records in their PEHR or being able to remove parts of the clinical information. People assumed the organization that held their PEHR would have full access to their personal information – and this was a concern. When asked for reactions to different types of organizations that might offer PEHRs, people expressed the most trust in health care provider organizations and little or no trust in health insurance companies and employers. Reactions to other organizations such as Google-Intuit were mixed.

Most of those we interviewed strongly favored giving patients the choice of signing up; many raised concerns about “opt out” approaches such as *Secure Network*'s. Those who objected to “opt out” noted the burden it imposes, the chance that some people might never hear about the choice of opting out, and the possibility that personal health information might be shared before people were able to opt out. A few people were neutral or positive about “opt out” because *Secure Network* was only for use by health professionals and because they felt it was in everyone's best interest to make health information readily available, especially for emergencies. Most people, including those who objected to “opt out” on principle, said that they personally would *not* choose to opt out of *Secure Network*.

Most people favored letting patients block some or all of their information on *Secure Network*, but couldn't imagine why anyone would want to. A few people thought blocking should not be allowed at all by *Secure Network* because withholding information could undermine a doctor's ability to provide quality

care. Most people said that they would not block their own information. A few people were concerned that mistakes might be made, such as blocking the wrong information. Some thought the procedure for complete blocking of information was too easy (just a phone call), and many people thought the procedure for selective blocking was too cumbersome. While being able to block *specific individuals* from seeing their health information was not important to most people, it was quite important to a couple of people for personal reasons based on actual experience. Overall, people thought it was good to let patients “unblock” their information if they changed their mind.

Conclusion

The findings summarized above indicate both a great opportunity and an urgent need for consumer education tools that help people understand the basics of health information exchange and the choices they have about participation.

Educating consumers will not be an easy task. The concepts and issues are complex and often unfamiliar. Consumers differ in knowledge, circumstances, literacy skills, computer skills and computer access. Given this diversity, consumer education will need to use a combination of tools and support, including written materials.

The materials we created for this project were well received by the people we interviewed. We are happy to share these materials and our lessons learned in testing them. We hope they will be useful resources for others who are working on consumer education tools.

FINAL REPORT

PART 1: Overview of this project

A need for consumer education tools

The rapid expansion of electronic health information exchange has created an urgent need for consumer education. Most people have only a limited awareness and knowledge of electronic health information exchange and what it means for them. To make fully-informed decisions in areas that affect them personally, they need specific and actionable information that is easy for them to understand and use.

Using methods such as opinion polling and focus group discussions, studies by the Markle Foundation and others have provided insights into the consumer's perspective on electronic health information exchange (Connecting for Health – Markle Foundation; National Consumer Health Privacy Survey, 2005; Westin, 2006). Most work has focused on policy issues and general research on consumers' knowledge, attitudes, and opinions. To date, little has been done to develop information materials or other education tools for use with consumers.

What did we do?

In late Spring 2007, the *Oregon Health Information Security and Privacy Collaborative* (Oregon HISPC) conducted a *Consumer Engagement Project*. We began by developing two types of consumer education tools. Written in plain language and illustrated with diagrams and examples, these tools explain basic concepts and describe two different scenarios of electronic health information exchange:

- A 16-page booklet about *Secure Network*, a fictional data-sharing service for use by health professionals (see Appendix C, page 33). *Secure Network* is not intended to be a model of how data should be shared. Rather, we invented *Secure Network* and its specific features as a means to test basic explanatory language and as a device to trigger consumers' reactions to issues such as opt out and limitations on patient access.
- A set of information sheets that outline key features of personal electronic health records (PEHRs) and contrast these features with those of *Secure Network* (see Appendix D, page 53).

When these tools were ready, we tested them by conducting 16 two-hour interviews with a demographically diverse group of consumers in the Portland metropolitan area and The Dalles. We used the interviews to collect consumer feedback on content, appeal, and ease of understanding the consumer education tools. We also explored consumers' reactions to the two contrasting scenarios they depict.

Who conducted this project?

This project was conducted by the Office of Oregon Health Policy and Research (OOHPR). Jody Pettit, MD, is Health Information Technology Coordinator, OOHPR. The project team included Oregon Health Care Quality Corporation, Portland State University, and the project consultants, McGee & Evers Consulting, Inc. For details on the project team, see Appendix A (page 30).

This project was funded by the Agency for Healthcare Research and Quality. We thank those who helped with this project by providing advice, feedback on draft versions of the explanatory materials for consumers, and assistance with recruitment of participants for the interviews. For acknowledgements, see Appendix B (page 31).

PART 2: Developing the consumer education tools

Scenarios and topics

Electronic health information exchange is complex and constantly evolving, and no single study could possibly address all concepts and variations that consumers might encounter. We were selective both in the issues we addressed and how we addressed them. In developing our prototype consumer education tools, we focused on areas of special interest to this project, which are (a) data privacy and security and (b) consumers' access to their own electronic health information and control over the ways in which it is shared.

To help stimulate wide-ranging discussion on these topics, we developed two consumer education tools. As outlined below, these tools describe scenarios that differ significantly, especially in terms of consumer access and control.

“Secure Network,” a fictional non-profit data sharing service for health professionals. Shown in Appendix C (page 33), the 16-page booklet about *Secure Network* tells consumers about this electronic data sharing service.

- It's important to keep in mind that *Secure Network* is *not* intended to be a model of how data should be shared. Rather, we invented *Secure Network* and its specific features as a means to test basic explanatory language and as a device to trigger consumers' reactions to issues such as data privacy and security, opt out, and limitations on patient access.
- *Secure Network* is designed for use by health professionals only. It facilitates the transfer of information from electronic medical records that are kept in different locations, but does not store any of the information in a database. It does not give patients direct access to information in their records, but shows them an inventory that describes what type of information is available to be shared. Unless patients take the initiative to opt out, information from their electronic medical records is automatically shared with any authorized health professional who requests it. The booklet describes the types of information that are shared and the safeguards for data privacy and security. For patients who want to opt out, the booklet tells how to block all or part of their information from being shared on *Secure Network*.

Personal electronic health records (PEHRs). Shown in Appendix D (page 53), the information sheets describe PEHRs. Some of the sheets make comparisons between PEHRs and *Secure Network*. PEHRs are described as being owned and controlled by the patient. Patients must take the initiative to sign up for a PEHR. They decide what information is included and they can add their own information and make corrections. Patients decide who gets to see information in their PEHR.

Development and revision

The education tools were written and designed by project consultants Jeanne McGee, PhD, and Mark Evers, PhD, McGee & Evers Consulting, Inc., who have extensive experience in health literacy and document design. They created these tools using guidelines for making written material clear and effective (McGee, 1999; McGee, forthcoming).

We circulated draft versions of the consumer education tools to project team members and outside reviewers and used their feedback to make improvements (for acknowledgments, see Appendix B, page 31).

PART 3: Collecting feedback from consumers

Interview participants

When the consumer education tools were ready, we conducted 16 two-hour interviews with consumers to get their feedback on these tools and to discuss issues related to electronic health information exchange.

The consumers we interviewed were a mix of women and men who ranged in age from their mid-twenties to their seventies. About half of them had a high school education and the others had up to four years of college.

Since our topic was about sharing of information from medical records, we wanted to interview people who would find this topic relevant to their own lives. To help ensure personal salience, we chose people who were above average in their use of health care services, based on the answers they gave to screening questions that asked about chronic health conditions, medical visits, emergency room visits, and hospitalizations.

For a detailed profile of interview respondents, see Appendix E (page 60).

Why did we use interviews instead of focus groups?

We chose to use interviews rather than focus groups because interviews are much better suited to the particular needs of this project.

In a typical focus group, each person has perhaps 10 minutes of total speaking time and people can be influenced or inhibited by what others say. In contrast, individual interviews allow each person to speak at length on many topics without being influenced or inhibited by others.

Moreover, as shown in the chart on the next page, interviews offer more privacy, flexibility, and a much broader range of methods for collecting in-depth feedback on written material.

	 Group sessions	 Individual interviews
Can you ask questions?	yes	yes
Can you have a group discussion that includes having participants comment on or build on what others say? . . .	yes	no
Can you observe what readers do with the material? . . .	limited	yes
Can you give readers tasks to see how well they can use the material? (“usability testing”)	limited	yes
Can you adapt the feedback session and your line of questioning based on how each reader reacts?	limited	yes
Can each reader speak at length on many topics?	no	yes
Can you give readers privacy (avoiding the influence of what others say, and making it easier to discuss sensitive topics)?	no	yes
Can you ask readers to “think aloud?”	no	yes
Can you concentrate on a single person without needing to manage group interaction?	no	yes

SOURCE: Jeanne McGee, McGee & Evers Consulting, Inc. (McGee, forthcoming).

Interview methods

Interviews were conducted in May 2007 in two Oregon locations. Nine interviews were conducted in the Portland metropolitan area and seven were done in The Dalles, a community of 12,000 in North Central Oregon. In Portland, we used a professional firm to recruit interviewees. In The Dalles, a project staff member handled the recruitment with assistance from a local clinic and others (see Appendix B, Acknowledgments, page 31).

The interviews took about two hours and participants were paid as a thank you for their time. The interviews were conducted by a two-person team of interviewer and note taker. There were three parts to the interview:

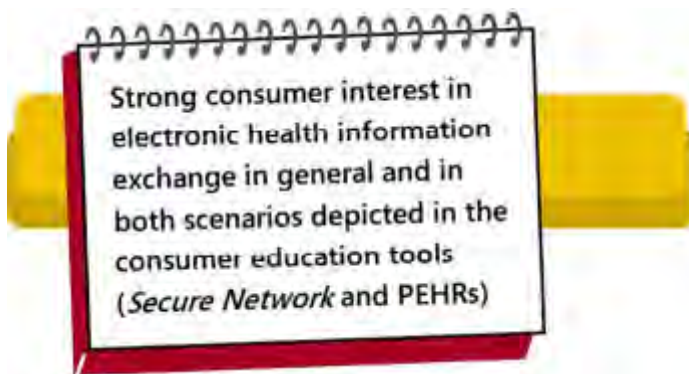
- *Secure Network*. The first part of the interview focused on the *Secure Network* booklet (shown in Appendix C on page 33), which describes a data sharing service that is designed for health professionals and offers consumers limited access and control. Using the booklet as an explanatory device, our interviews explored consumers' understanding of basic concepts of electronic health information exchange and sought their reactions to specific features of the approach taken by *Secure Network*.
- PEHRs. The second part of the interview focused on PEHRs and explored consumers' reactions to features that expand the patients' access to and control over the sharing of their health information. This discussion used separate information sheets as a device to illustrate some of these features and to make comparisons to the *Secure Network* (see Appendix D on page 53).
- General discussion. The last part of the interview included questions about how much importance people placed on such things as having the opportunity to stop specific types of information from being shared, to prevent specific health providers from seeing their records, and to be able to add information to their health record. Other topics were addressed as well, such as asking how people would feel about having a consolidated copy of their electronic medical records managed by a third party, and which types of organizations they would trust to be the third party.

To get feedback on the consumer tools and explore people's opinions about electronic health information exchange, the interviewers used a variety of techniques (McGee, forthcoming). Throughout the interview, participants were encouraged to read the materials at their own pace and share whatever thoughts or questions came to mind by making comments aloud. To help assess comprehension, interviewers periodically asked people to talk in their own words about what they had just read. Using follow-up questions, interviewers probed to learn more about people's spontaneous reactions and to gain insights into how they were interpreting and reacting to the consumer education tools.

By showing detailed written explanations of basic concepts, we were able to explore questions that arise spontaneously when people begin to understand more fully what is involved in electronic health information exchange. We were also able to identify aspects of electronic health information exchange that tend to be difficult for people to understand or prone to misinterpretation.

PART 4: TOPIC-BY-TOPIC findings with illustrative quotations from the interviews

Strong consumer interest but limited knowledge and understanding



There was strong consumer interest in electronic health information exchange. Interviewees saw value in making information from their medical records readily available when needed, especially during emergencies, when they travel, and when they see a new doctor.

Responding to the booklet about *Secure Network*, interviewees saw value in having an electronic health information service that was designed for use by health professionals. Responding to the information sheets, they particularly liked the consumer access and control provided by a PEHR.

Several people commented that it would be more accurate to have their records available than to rely on their own memories of care they had received. They also felt that electronic health information exchange would provide a more complete medical record. In particular, people with extensive medical records loved the idea of having all of their health information readily available to their health professionals. A few of them had already taken considerable effort to assemble copies of their medical records on their own.

The issue of cost and who would pay was not addressed in either the booklet or the information sheets. During the interviews, a few people brought up this topic, wondering what the data sharing services or PEHRs would cost and who

would pay. A couple of people speculated that this type of information exchange might raise the cost of care for patients.

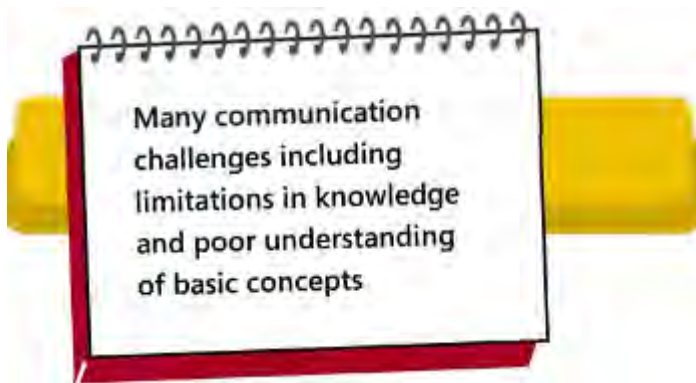


"Is this free? Or is it something I'd have to pay for? Because that would make a difference to me. Basically, they should tell right away who funds it."

Secure Network was described as being a non-profit company created by Oregon health insurance plans, hospitals, employers, state government, and doctors. Several interviewees commented favorably on *Secure Network's* non-profit status.



*After reading that Secure Network is a non-profit organization:
"Non-profit.. [it's] good to know there's not money to be gained and there's less reason to do things that aren't appropriate. Local involvement is good. The insurance plans concern me - but [they are] probably hard to exclude."*



While the interviews showed strong consumer interest in electronic health information exchange, they also revealed serious communication challenges. The concepts and mechanisms of electronic health information exchange are complex and unfamiliar to most people – even to people with computer skills and first-hand familiarity with the information in their medical records.

Nearly everyone we interviewed was a computer user. In fact, all but one person had used the internet to search for health information. Many of the people had chronic conditions and extensive medical histories; several had personally assembled a personal file of copies of information from their medical records. Nonetheless, most of them knew very little about electronic medical records or electronic transfer of health information, and they had some misconceptions.

- Overall, the mechanics of electronic data storage-retrieval- transmission were very poorly understood. Most people knew enough to raise some questions and concerns, particularly about the threat of hackers and identity theft, but overall, much of electronic health information exchange was essentially a “black box.” They were interested in learning more, but the “electronic” part was abstract and difficult for them. They were accustomed to seeing paper records and many seemed to have great trouble visualizing electronic versions and could not imagine electronic records being stored, updated, and transmitted.
- Limited knowledge also made it hard for people to put the topic of electronic health information exchange into a broader context. People knew very little about the multiple ways in which their health information is now being stored and being routinely shared for various purposes including processing of payments for care and quality assurance, sometimes with their knowledge and permission and sometimes not. For example, several interviewees emphasized that they didn’t want their health insurance company to see any of their personal health information.
- People made different assumptions and interpretations. Readers are not just passive receptacles of information – they actively interpret what they read in the light of their own knowledge, interests, and experiences. Consequently, the same information in the booklet or information sheet sometimes means different things to different people. For example, the booklet says, “In general, the patient information that is shared on *Secure Network* is for care provided during the last three years.” Most interviewees focused on how this time period seemed too short:, and they had no idea about why:



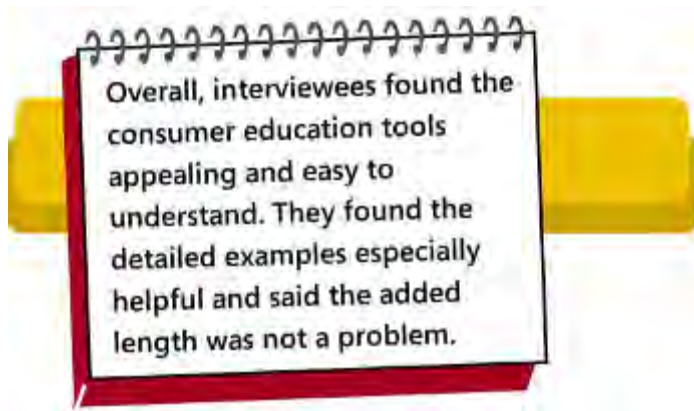
“Peoples’ care might have slipped through the cracks, so their last three years could be almost a blank, & might not include some important information.”

But there were a couple of interviewees who were much more knowledgeable and they were able to speculate about reasons for this short time frame:



“One possible reason is] paper being the predominant form before just recently. Probably, computer medical records don’t go back so far. And it would take a lot to search out everything [and scan in all the paper records from years ago].”

Reactions to the project's consumer education tools



Overall, interviewees reacted very positively to the booklet and information sheets. They made many positive comments about language, layout, illustrations, colors, and friendly tone. They called the materials “user friendly” and “easy to read.” They especially liked the examples.

Results from the interviews showed that the booklet and information sheets worked well in helping consumers understand some important points about electronic health information exchange. Most people were able to sum up the main points of various sections in their own words. For some topics, there was occasional confusion or misinterpretation. For example, it proved particularly difficult to get across the notion that blocking one’s information on *Secure Network* does not block the same information from being shared in other ways.

Based on comments made by the interviewees, the following features helped make the booklet and information sheets easier for people to understand and use:

- Starting with the most basic points, such as what is a medical record, what is meant by “electronic,” and what is the difference between paper records and electronic records. (See page 1 of the booklet, which appears on page 37 of this Final Report, in Appendix C). This was new information to some people. During the interviews, we checked to see whether people who already knew these basics would be put off by the explanations we included. They said they were not, in part because the material was designed in a way that made it easy for them to skim and read selectively.
- Raising and answering questions that came up in some people’s minds as they were reading. Below is an example from the booklet:



How can you tell whether your medical records are being kept in folders or computer files?

It can be hard to know whether your medical records are being kept in folders or computer files. *If you don't know, just ask.*

- Using simple words that people already knew. For example, the booklet uses the term “blocking all of your information” instead of “opt out.” Although one person used the term “opt out” when making a comment, everyone understood what was meant by “blocking.”
- Explanations that included embedded definitions of technical terms. Here is an example from the *Secure Network* booklet that shows an embedded definition of “diagnostic images.”

Diagnostic images

- “Diagnostic images” are like pictures of the inside of your body. Examples are x-rays, ultrasounds, mammograms, MRIs, and CT scans.
- The information about diagnostic images that is shared on *Secure Network* includes a report about what the image means. Often the image itself (such as an x-ray) can also be sent electronically using *Secure Network*

The *Secure Network* booklet explains several concepts that are unfamiliar, complex, and non-intuitive. For example, these include explaining how *Secure Network* transfers information but does not store it in a data bank, and explaining what patients must do if they want to block a specific part of their information from being shared on *Secure Network*.

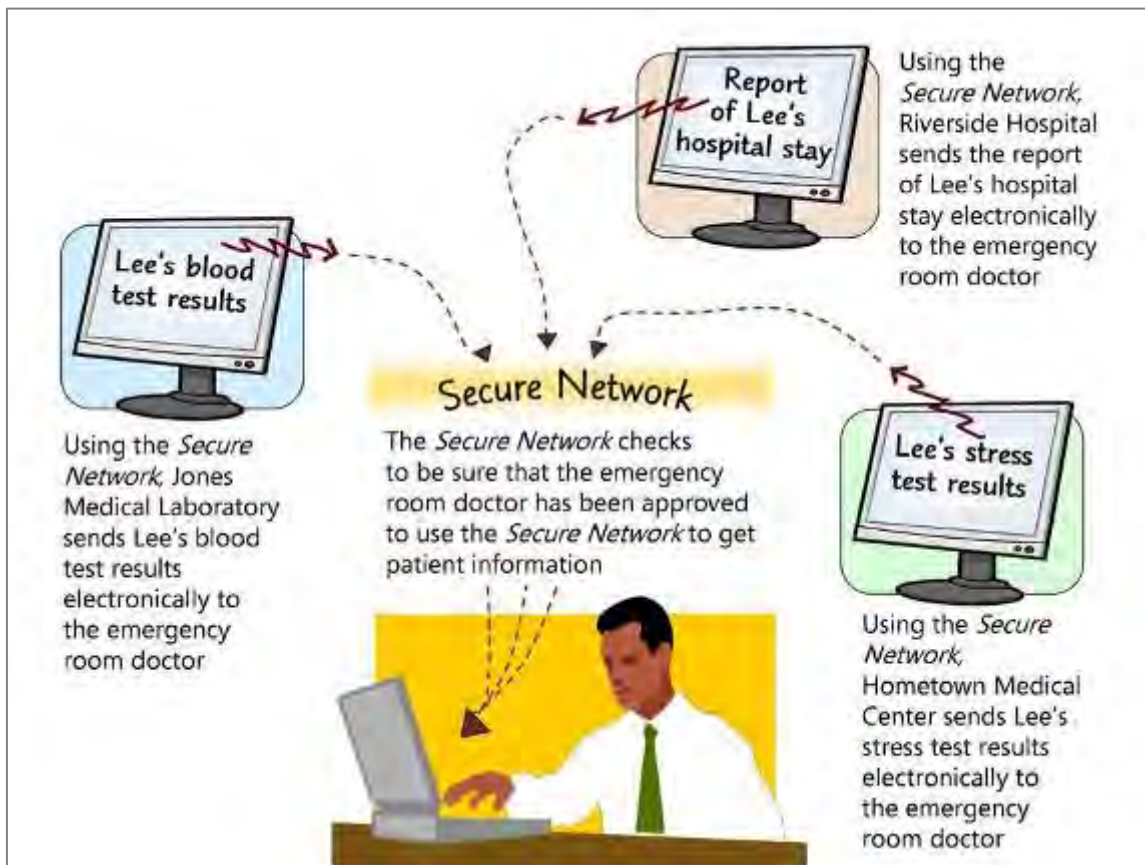
To help explain these difficult concepts, the booklet uses detailed examples. Interviewees emphasized the importance of the detailed examples in the booklet, calling them extremely helpful.

For example, when they first started reading the booklet, most people assumed that *Secure Network* was a centralized data bank of health information. This

made sense, because the concept of a centralized data bank is more intuitive and familiar than a data sharing service that does not keep copies of the information it shares. As they continued to read about *Secure Network* and what it does, some people became confused:

"At first, I figured they were entering the information, but now I see it saying that Secure Network doesn't keep any of the information. So what's going on?"

For many people, the detailed example shown below helped clear up their confusion.



Here are two examples of comments that people made in response to this detailed example:



"I like this illustration because it really shows how {Secure Network} is not a data bank - it's just retrieving information."



“What I’m getting from this is that the network is only a channel. No huge room full of data. Not a source of information, just a vehicle [for delivering information].”

Other examples that people especially liked include the list of information about Ed (Appendix C, page 46) and the full page step-by-step example that shows what Anna must do to block her blood test from being shared on the *Secure Network* (Appendix C, page 51). In the information sheets on PEHRs, people especially liked the example of types of information Lee might want to add to her PEHR (emergency contact information, name and phone number of her family doctor, and information about her family health history, immunizations, and allergies to medications).

Including detailed examples made the booklet longer. We knew from people’s comments that the examples were helpful. But to check on whether the added length was a problem, interviewers asked whether people thought the booklet was “too short, too long, or about right.” Although the booklet was 16 pages long, 14 of the 16 participants said the length was “just right.” A couple of them said that it seemed a bit long to them when they first saw it, but then once they started reading, it was so easy to understand that they didn’t care about the length.

Protecting privacy and security of the information



Data privacy and security were major concerns; people wanted to know about specific safeguards. People raised concerns about identity theft, unauthorized access, and possible misuse of their information. Recognizing that no system can be perfect, they were reassured by the safeguards described in the booklet. In particular, they liked that *Secure Network* (a) keeps track of who sees their information and makes a report of who has seen their information available to the patient; (b) requires users to be trained and sign confidentiality pledges; (c) tells them if security is breached and (d) punishes anyone who

breaches security. Several people thought there should be oversight by an outside, independent organization.

Data privacy and security were major concerns to the people we interviewed. These concerns came up early in the interview, both as spontaneous reactions to the general topic of electronic health information exchange and in response to the specific discussion of data privacy and security safeguards in the booklet about Secure Network.

- Many people focused mainly on the threat of identity theft and gave examples from the news or personal experience.
- People raised issues about unauthorized access or possible misuse of their information. For example, a couple of people were worried that non-providers such as administrative people or someone passing by an unattended computer screen could have easy access to their information. (A few people noted that unauthorized access or misuse of information is also an issue for paper medical records.)



"[What if] my next door neighbor works for Secure Network and looks me up?"

- A few suggested there should be oversight by an outside, independent organization. Bank audits were mentioned as an example.
- A few people were uneasy in general about reliance on computers, expressing concerns about possible loss of information.



"They shouldn't keep everything on computers - what if it gets blitzed out. . . I'm not a computer person . . . but I think they should keep two sets of records -- one on paper and one in the computer."

Overall, most people were fairly comfortable with the data privacy and security procedures described in the booklet about *Secure Network*.

- Recognizing that no system can be perfect, they were reassured by specific safeguards described in the booklet. In particular, they liked that *Secure Network* (a) keeps track of who sees their information and will tell them; (b) requires users to be trained and sign confidentiality pledges; (c) tells them if security is breached and (d) punishes anyone who breaches security.



After reading the description of Secure Network's security procedures (Appendix C, page 47) "Seems like they've covered all the bases and done what they could. Still, nothing is foolproof."



After reading that patients could get a list that tells who has used the Secure Network to look at their information (Appendix C, page 47) "Now that I've read this, it makes me feel more safe. That they would show me what transpired ... that sounds really good. [It makes me] more ready to trust them."

- Several people thought the procedures sounded good, but couldn't picture how Secure Network would implement them. For example, they wondered how Secure Network would *really* be able to tell who it was who was using the network to get information.



"But how will they identify patients? Because what they might ask for is the same information you need to steal someone's identity."



"The booklet talks a lot about the doctors using Secure Network and how they must be trained and how they must agree to follow the confidentiality rules. All well and good. But I think that the booklet should state how Secure Network knows who my doctors are or will be. If my PCP refers me to the orthopedist ... how does Secure Network know to [let the orthopedist] look at my record? "

- For a few people, finding out that Secure Network was not a centralized data bank gave them a greater sense of security.



"It's good to know that {the Secure Network} is not a database, so all your information isn't sitting in one place where someone can hack into it."

Views about who should see the health information



When they read the booklet about *Secure Network*, interviewees were happy to see that the information sharing was specifically for clinical use and restricted to health care professionals. They were eager to give health professionals easy access to their health information and *Secure Network* seemed like a valuable service to them.



"[Secure Network] sounds like a good idea. . . . To have it open and available to the medical profession but not accessible to anyone who might want to snoop."



{After reading that doctors are allowed to put copies of information they receive through Secure Network into the medical records they keep for the patient} "This could save someone else the trouble: it's good that it goes into the records."


Occasionally interviewees would share stories of problems they had experienced with medical care. But overall, they made numerous comments that reflected great confidence and trust in their health care providers and how they would use electronic health information.

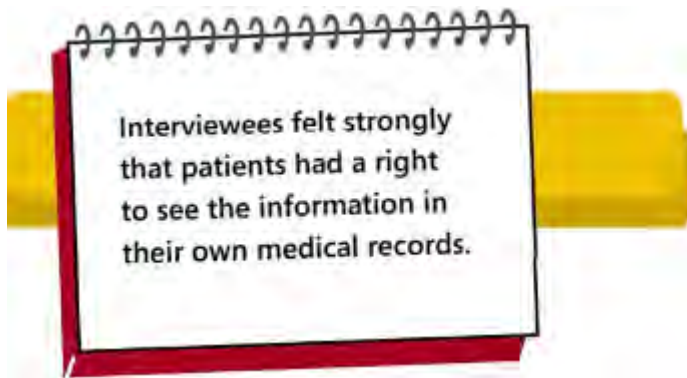


"[There's a lot] of trust between doctors and patients, and doctors have an oath that's outside of Secure Network."

The booklet on *Secure Network* included the text shown below, which gives specific exclusions. Interviewees were pleased and reassured to learn that

certain organizations such as health insurance companies were not allowed to use *Secure Network* and that *Secure Network* could not be used to get patient information for purposes of processing payment or fund raising.

- 
- Doctors and other health professionals who are providing your care are the only ones allowed to see the information about you**
- The *Secure Network* Company does not allow anyone to use the *Secure Network* to sell you things or ask you for money.
 - The *Secure Network* Company does not allow anyone to use the *Secure Network* to handle payments for your care.
 - f Organizations such as health insurance companies need certain types of information about your medical care in order to handle payments for your care. They get this information about your medical care in other ways that do not involve using the *Secure Network*.
 - *Secure Network* does not allow employers, life insurance companies, drug companies, or other companies to see any information about you that is shared using *Secure Network*.
 - f These organizations may have other ways to see your personal health information that do not involve using the *Secure Network*.



Most people we interviewed thought patients had the right to see the information in their medical records and that access would not be a problem. They assumed that patients who wanted to see information in their medical records could simply ask and their health providers would show it to them. Some of them with extensive medical histories had already obtained copies of their own records to make it easier when they saw a new provider.



"It's a big advantage for patients to have full access if they want it. It was very important to me to see my own records. I think most people wouldn't want to read them. Others want to muddle through the records at home in their own space, and they could ask their doctors if they had questions."



"It's about them, so they should be able to see it"

A couple of people noted that patients would reviewed their own records would be good at spotting certain kinds of errors ("hey, I never broke my arm. . .why is that in here?").

Others, like the one quoted below, pointed out that by looking at their records, patients might learn more about the care they were being given.



"See your own information? Yes, I think you should be able to. I [wasn't told about some tests they did]. .I don't ask a lot of questions [and I only found out about these tests when I saw my medical records]."

Interviewees acknowledged that medical records can be very technical and difficult for consumers to understand. They thought patients might need to get some help in understanding the information in their own records.



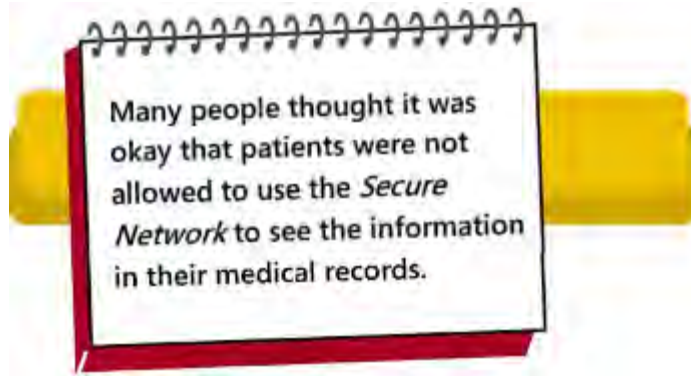
(After reading that patients cannot use Secure Network to see the information in their medical records)

"I wonder why you can't see your own medical records. It's about you... You may not be able to understand it, of course."

(Follow-up by interviewer: "Would that be a good enough reason not to let patients see it?")

"No.."

As we discuss in a later section, people were very positive about PEHRs because PEHRs give patients full access to their health information.



As we've already noted, most interviewees strongly favored letting patients see the information in their own medical records. However, many of these same people who favored patient access thought it was okay that *Secure Network* does not let patients use the *Secure Network* to see their own records. For these people, giving doctors easy access was the key issue.

They wanted patients to have access as well, but they reasoned that patients could use some way other than *Secure Network* to get access, such as asking their providers for the information. This meant that restricting patient access to *Secure Network* was not the same as restricting patient access altogether.



"It doesn't bother me that the patient can't see the details [of their medical records on Secure Network] because hopefully the patient already knows."



"If you want to know the details, you can always ask the doctor, and that's sufficient."

While many interviewees did not object to *Secure Network's* restriction on patient access, there were a few people who thought it was actually *best* for *Secure Network* to restrict patient access. One reason was to help protect against identity theft and possible misuse of information.



"I like it that [patients] can't see all the details because someone else could see the details of your medicines and then try to get a refill."

A couple of people thought restricting patient access would help protect the privacy of teenagers' personal health information by preventing inappropriate access by their parents.

Finally, a few people thought that getting the information directly from their providers would work better for patients than giving them independent access through Secure Network. They reasoned that patients would need some help in understanding the information and could get that help from their provider.

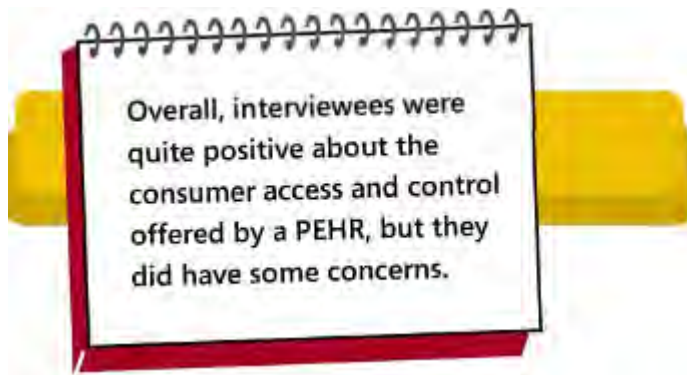


"I really think it's better to have it the way it is here [in the booklet]. If you saw everything in your file, you might freak, and then you'd be calling your doctor anyway."



I don't think I should be able to see it by logging on at my house, but I should be able to see it when I'm at the doctor's office.

Controlling whether information is shared and who can see it



Overall, people were very positive about PEHRs because PEHRs give patients full access to their health information. They liked that patients would be the ones to decide whether or not to have a PEHR, and that patients could add their own health information to their PEHR. They liked the idea of a patient having control over how the information would be shared, including the option to make their health information available to trusted family members or friends.

When people saw the description of PEHRs in the information sheets, some expressed concern that patients would be allowed to make changes to their own medical records in their PEHR or being able to remove selected pieces of clinical information.

Specifically, the first information sheet on PEHRs, titled “What is a ‘personal electronic health record?’” includes the following heading “You are the one who ‘owns’ and manages this personal health record.” Under this heading, bulleted points highlight various features of a PEHR. Two of these bulleted points are reproduced below:

“You decide which information from your medical records should be included in your personal health record. If you want to, you can remove certain information.”

“You can add notes or comments to your personal health record, such as adding comments on some of the health information it contains.”

In general, people were okay with patients adding their own information, but they worried that if patients made changes to the clinical information, they could mislead providers and jeopardize their care. One person joked about how this was his opportunity to make his cholesterol numbers look much better than they really are.



“Giving people more control over access by others carries some risk. What if there’s something in that blood test that would help the doctor and then the patient would block it? Seems like a problem. And anyway, presumably there’s a record somewhere that can’t be changing or blocked.”



“Sometimes keeping track of all your test results can be really hard. It would be good for the patient to have full access (but not necessarily to be able to change any of it). Would be nice to have it be secure, be confident nobody’s attaching things, and so on.”

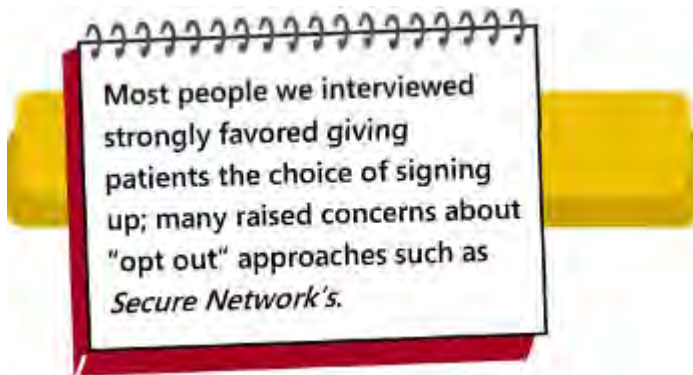
Based on comments they made, it seemed that some people were confused about whether anyone would be able to tell where patients had made additions or corrections to their PEHRs. They had trouble envisioning how a patient’s own entries might be labeled so they would be distinguishable from lab reports and other clinical information in the personal health record.

People assumed that the organization that held their PEHR would have full access to their personal information – and this was a concern. When asked for reactions to different types of organizations that would offer PEHRs, people expressed the most trust in health care provider organizations. They expressed little or no trust in health insurance companies and employers.



“If you’re having mental health problems, can your employer find out and use it against you?”

People had mixed reactions to other possible sponsors of PEHRs. For example, interviewers briefly described the collaboration of Google and Intuit as one possible sponsor. Several participants expressed confidence in the systems knowledge and security safeguards that these companies could provide, but they had questions about their health-related expertise. Overall, interviewees were more trusting of health care provider organizations such as hospitals and medical groups.



In this project, we wanted to explore how people feel about consumer control over participation in an electronic health information sharing system. When we were creating the booklet about the fictional *Secure Network*, it made sense to describe *Secure Network* as an “opt out” system:

- Making *Secure Network* an opt out system gave us the opportunity to develop and test ways of explaining what is meant by “opt out” and giving instructions about how to do it. Opting out is more complex and less intuitive to consumers than a sign up procedure or consent form that would be used for opting in. By focusing on explaining opting out, we felt that our project would make a greater contribution to the development of consumer education tools.
- We anticipated that consumers would generally be supportive of an opt in system that asks people to sign up and give permission for their health information to be shared. But how would they feel about a system that does not offer this upfront choice to sign up? To help find out, we made *Secure Network* an opt out system. Unless patients take the initiative to opt out, information from their electronic medical records is automatically shared on *Secure Network* with any authorized health professional who requests it.

For easy reference, here’s an excerpt that shows the first part of the explanation given in the *Secure Network* booklet:

Your information will be shared on the Secure Network unless you “block” the sharing



- ▶ The Secure Network Company **assumes** that **you agree** to have your information shared electronically on Secure Network -- unless you say “no”
 - If you are okay with having information from your medical records shared electronically using Secure Network, you do not need to do anything. The Secure Network Company will keep on allowing your information to be shared on the Secure Network.
 - If you are **not** okay with having information from your medical records shared electronically using Secure Network, you must follow the instructions below that tell how to block your information.

In general, the interviews showed a strong preference for “opt in” rather than “opt out.” Most interviewees thought it was appropriate to give people the choice of signing up for a health information sharing system rather than enrolling them automatically and then making them take the initiative if they didn’t want to participate. Here are examples of their reactions:



“Ethically wrong - how could it be legal? . . . I want to say yes before it starts!”



“[It sounds like this is saying that] I don’t have to give permission for all this information to be shared. . . . But who did give the permission? . . . It sounds like the whole medical world is able to access my information. How can this be true? . . . They need to tell more about this!”



"I'd rather check a box that says I'm giving permission. They shouldn't be assuming I'm OK with it, they should be assuming that I'm not. . . .I don't want to have to read the fine print to find out I needed to opt out of something."



"Will there be a consent form for patients to say it's okay? Will it be like a . . . health insurance release? Would you sign up for it with each doctor you see? Maybe there would be a [special] provision for the ER. "

Those who objected to "opt out" raised a variety of concerns, including the burden involved in blocking the information, the chance that some people might never hear about the choice of opting out, and the possibility that personal health information might be shared before people were aware of it and able to and able to opt out.



"[It's a] slippery slope . . . No matter how much you advertise on TV or whatever. . . [there] will still be some people who never know [about their choice to opt out]."



"This would be good if everybody wants to be on it. But what if you don't know that the network has already started? And would there be a physical consent form to be signed? Like something you'd hear about at the doctor's office? Especially because some people might not take the time to block their information."



"It's unrealistic to think doctors and nurses would have the time and ability to explain about this network to patients."

A few people either saw no problem with "opt out" or favored having it this way. They felt okay about opt out because *Secure Network* was only for use by health professionals. Several mentioned that it was in everyone's best interest to make health information readily available, especially for emergencies.



"[Not having patients give permission first] is okay as long as Secure Network is used only by health professionals - [they're] saving lives. . . You don't want bureaucracy to get in the way."

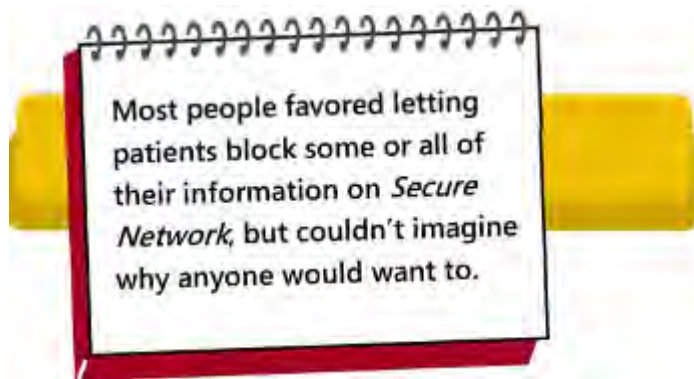


"I don't think it's necessary for Secure Network to ask people whether they should be in or not. I think everyone should be in for their own safety."

Most people, including those who objected to "opt out" on principle, said that they personally would *not* choose to opt out of *Secure Network*.



"I like that you can block the information. Me personally, I wouldn't feel the need to opt out, unless there was a security breach."



Most people we interviewed thought it was a good idea in general to allow blocking of information on *Secure Network*. Many of these same people commented that they would not want to block any of their own information, and they did not see why anyone would want to.

A few people thought blocking should not be allowed at all by *Secure Network*. They felt that making the information available was in the patient's best interest. They also felt that selective blocking, in particular, could undermine a doctor's ability to provide quality care by withholding information the doctor should know.



Giving people more control over access by others carries some risk. What if there's something in that blood test that would help the doctor, & then the patient would block it? Seems like a problem. And anyway, presumably there's a record somewhere that can't be changing or blocked."



"As long as it's only being seen by doctors and health professionals, I see no reason for blocking [any information]."



When the person wants to sign up for the program, there should be [something to tell them about the rules]. They shouldn't be able to block things and they should be told that they can't block it at the beginning."

A few people were concerned that mistakes might be made, such as blocking the wrong information.



"What if you call in and say you want it blocked and [then they] block the wrong thing? . . . How would I know what they actually blocked?"

A few found the procedure for *completely* blocking of all information on *Secure Network* too easy. They thought it should require a signature, not just a phone call.



"This almost seems too easy. You shouldn't be able to just call up and tell them. You should have to sign something. Some doctors won't even fax you something!"

Some people found the procedure for *selective* blocking of specific information too cumbersome. It required people to go directly to the source of the information and ask that source to stop making the information available on *Secure Network*. A few suggested it would work better if patients could block selected information right when they were about to receive the care.



"If you have a lot of records you don't want people to see, you'd have a lot of places you'd have to contact. Not so good. Why can't it be simpler?"



{After reading the example of how Anna blocks one piece of information from being shared by calling the source that holds that information; "[So Anna] has to tell the place that has the blood results to stop sending - that's too much! There could be mess-ups all over the place, if you ask me."



"There should be a way . . . when I get a test, to say "yes" or "no" to Secure Network at that very point.[This would be] a little bit of trouble, but would save time in the long run."

A couple of people wanted to be able to block their information on a case-by-case basis, as the need for information might arise. (This option was not offered by *Secure Network*.)

The booklet gave people the option of blocking part or all of their *information* from being shared on *Secure Network*, but it did not offer the option of blocking particular *individuals* from seeing the information. When interviewers asked whether it would be important to be able to block specific individuals from seeing their health information on *Secure Network*, most people said no. However, being able to block specific individuals from seeing their health information was quite important to a couple of people for personal reasons based on actual experience.

The booklet explains that people can ask to have their information “unblocked” if they change their mind later on. Overall, interviewees liked the idea of being able to unblock information.

Conclusion

Findings from our in-depth interviews showed that consumers were interested in electronic health information exchange but knew very little about it. While the concepts, mechanisms, and administrative aspects of electronic health information exchange were complex and hard for them to understand, they were intrigued and receptive to learning more. The people we interviewed were also deeply concerned about the privacy and security of their medical records and possible misuse. Most felt that patients should give permission before their health information is shared on a network. They wanted information and reassurance about how they would be protected from identity theft and other privacy or security breaches, and they wanted those who are involved in electronic health information exchange to be accountable.

Taken together, these findings indicate both a great opportunity and an urgent need for consumer education tools that help people understand the basics of electronic health information exchange and the choices they have about participation.

Educating consumers will not be an easy task. The concepts and issues are complex and often unfamiliar. Consumers differ in knowledge, circumstances, literacy skills, computer skills and computer access. Given this diversity, consumer education will need to use a combination of tools and support, including written materials.

The materials we created for this project were well received by the people we interviewed. We are happy to share these materials and our lessons learned in testing them. We hope they will be useful resources for others who are working on consumer education tools.

References

Connecting for Health -Markle Foundation

Connecting for Health was created by the Markle Foundation and is led and managed by Markle. The collaborative is funded by both Markle and the Robert Wood Johnson Foundation. For conference proceedings and other materials, visit <http://www.connectingforhealth.org/> and www.markle.org

McGee, Jeanne

1999 *Writing and Designing Print Materials for Beneficiaries: A Guide for State Medicaid Agencies*. Written for the Centers for Medicare & Medicaid Services (CMS), formerly known as Health Care Financing Administration (HCFA). Baltimore, Maryland: HCFA Publication Number 10145, October 1999.

Forthcoming *Toolkit for Making Written Material Clear and Effective: A Health Literacy Resource from the Centers for Medicare & Medicaid Services (CMS)*. Toolkit Part 4, "Understanding and using the Toolkit Guidelines for Writing," pages 1-96; Toolkit Part 5, "Understanding and using the Toolkit Guidelines for Graphic Design," pages 1-219; Toolkit Part 6, "How to collect and use feedback from readers," pages 1-257. (NOTE: This is a revised and expanded edition of McGee, 1999. It is currently undergoing final review and clearance by the government and will be distributed in PDF format on a website.)

National Consumer Health Privacy Survey

2005 Conducted for the California Healthcare Foundation by Forrester Research, Inc. <http://www.chcf.org/topics/view.cfm?itemID=115694>

Westin, Alan

2006 Privacy and EHR Systems: Can we avoid a looming conflict? Presentation to Markle Conference on Connecting Americans to their Health Care, December 7-8, 2006, Washington, D.C. (http://phrconference.org/conf_resources/presentations/dec7/improving_access.pdf)

APPENDIX A

Project Team

Office for Oregon Health Policy and Research (Salem, Oregon)

Jody Pettit, MD
*Health Information Technology Coordinator
HISPC Project Director
(Director of this project)*

Summer Boslaugh, MBA, MHA
HISPC Project Manager

Dawn Bonder, JD
*HISPC Project Manager (assisted with recruitment of interview participants
in The Dalles)*

McGee & Evers Consulting, Inc. (Vancouver, Washington)

Jeanne McGee, PhD and Mark Evers, PhD
*(Wrote and designed the explanatory materials; conducted the consumer
interviews; wrote this final report)*

Portland State University (Portland, Oregon)

Matthew Carlson, PhD
*Associate Professor, Department of Sociology
Principal Investigator
(Provided consultation for the development and implementation of the
consumer interviews)*

Oregon Health Care Quality Corporation (Portland, Oregon)

Nancy Clarke
*Executive Director
(Provided consultation for project design and implementation)*

APPENDIX B

Acknowledgements

We are grateful to Josh Lemieux and the Markle Foundation for sharing their knowledge and expertise and providing advice to this project:

Josh Lemieux
Director
Markle Foundation Information Technology Project
(The Markle Foundation is in New York City; Josh Lemieux is based in Portland, Oregon)

Reviewers:

Thanks to the following people who reviewed early drafts of the explanatory material for consumers and provided helpful suggestions for improvement:

Chris Apgar, CISSP
President
Apgar & Associates, LLP
Portland, Oregon

Carol Cronin, MSW
Consultant
Annapolis, Maryland

Chris DeMars, MPH
Program Officer
Northwest Health Foundation
Portland, Oregon

Joyce DeMonnin, MPH
Director of Public Outreach
Oregon AARP
Clackamas, Oregon

Joyce Dubow
Senior Advisor
Office of Policy and Strategy
AARP
Washington, DC

Sydney E. Edlund
Project Analyst
Providence Health System
Portland, Oregon

Dick Gibson, MD, PhD, MBA
*Senior Vice President and Chief
Information Officer*
Legacy Health System
Portland, Oregon

Bob Joondeph
Executive Director
Oregon Advocacy Center
Portland, Oregon

Deborah Nedelcove, DC, MHA, CPHQ
Vice President
Risk Management
Avamere Health Services
Wilsonville, Oregon

John Richardson
Director, Privacy and Security Policy
Digital Health Group
Intel
Hillsboro, Oregon

Ken Provencher, MBA
Chief Executive Officer
PacificSource
Eugene, Oregon

Margaret Smith-Isa
Program Development Coordinator
Public Employees' Benefit Board
Salem, Oregon

Assistance with Recruitment for Consumer Interviews

We are grateful to the Columbia River Women's Clinic in The Dalles, Oregon, for allowing us to conduct consumer interviews at the clinic.

In addition, we thank the following people for their help in recruiting participants for the consumer interviews conducted in The Dalles:

Laurie Miller
Manager
Columbia River Women's Clinic
The Dalles, Oregon

Thomas Hodge, MD
Internal Medicine
Mid-Columbia Medical Group
The Dalles, Oregon

Tracy Carver, MPA
*Community Partnerships and Self-
Management Coordinator, Oregon
Asthma Program*
Oregon Public Health Division
Portland, Oregon

Virginia Shaw-McClain, RN, CDE
Diabetes Nurse Educator
Mid-Columbia Medical Center
The Dalles, Oregon 97058

Holli Elton, RN, BSN
Chronic Disease Management
Mid-Columbia Medical Group
The Dalles, Oregon

APPENDIX C

“Secure Network” booklet

This appendix shows the explanatory material used in Part 1 of the consumer interviews

This appendix shows a 16-page booklet about *Secure Network*, a fictional data-sharing service for use by health professionals. Please note that *Secure Network* is not intended to be a model of how data should be shared. Rather, we invented *Secure Network* and its specific features as a means to test basic explanatory language and as a device to trigger consumers’ reactions to issues such as opt out and limitations on patient access.

At the beginning of the interviews to get feedback on this booklet, consumers were told that *Secure Network* was “a non-profit organization created by Oregon doctors, health insurance plans, hospitals, employers, and state government.” Interviewers stressed that it was not a real organization.



Giving health professionals better access to your medical records so they can give you better care

The Secure Network is a non-profit service for sharing patient medical records that are kept in computer files and stored in different locations.

Your doctors and other health professionals can use the Secure Network to get quick and easy computer access to information from your medical records.

This booklet explains things you need to know about the Secure Network. It also tells what you must do if you want to block your information from being shared on the Secure Network.





Contents of this booklet

Introduction

About your medical records.....	1
The Secure Network - what is it for?	2
Using the Secure Network can help your doctors and other health professionals give you better care.....	4

The Secure Network – how does it work?

The Secure Network - an example to show how it works.....	4
What kinds of information from your electronic medical records can be shared by using the Secure Network?	8
Who can use the Secure Network to see information about you?	9
Are <u>you</u> allowed to see the information about you that is being shared on Secure Network?	9

How does Secure Network protect your privacy?

How does Secure Network protect the privacy and security of your health information?	11
--	----

Is it okay with you to have your medical records shared on Secure Network?

Your information will be shared on the Secure Network unless you “block” the sharing.....	12
How to block all sharing of your personal health information on the Secure Network.....	13
How to block only part of your information from being shared on the Secure Network.....	14

Do you have any questions or concerns?

How to contact the Secure Network if you have questions or want to make a complaint.....	15
--	----

About your medical records

What are your “**medical records**”?

Your medical records contain information about your health history and the medical care you have received. These records might include:

- Notes written by doctors, nurses, and other health care professionals you have seen.
- Information about your office visits, test results, prescription medicines, x-rays, hospital stays, mental health counseling, physical therapy, and other care.
- Information about your family medical history, immunizations, and medication allergies.

You get your care in different places and **each place keeps its own records** of your care

The medical records with information about your health history and medical care might be stored in many different places. For example:

- All of the doctors and other health professionals you have seen keep their own records of your care.
- The places where you have had lab tests, x-rays, visits to the emergency room, hospital stays, or filled a prescription for medicine also keep their own records of your health information.

Your medical records might be kept in **filing cabinets** or in **computer files**



Many medical records are kept in filing cabinets

When your personal health information is on sheets of paper, it's called “**paper medical records**.” Paper medical records are put into folders and kept in filing cabinets.



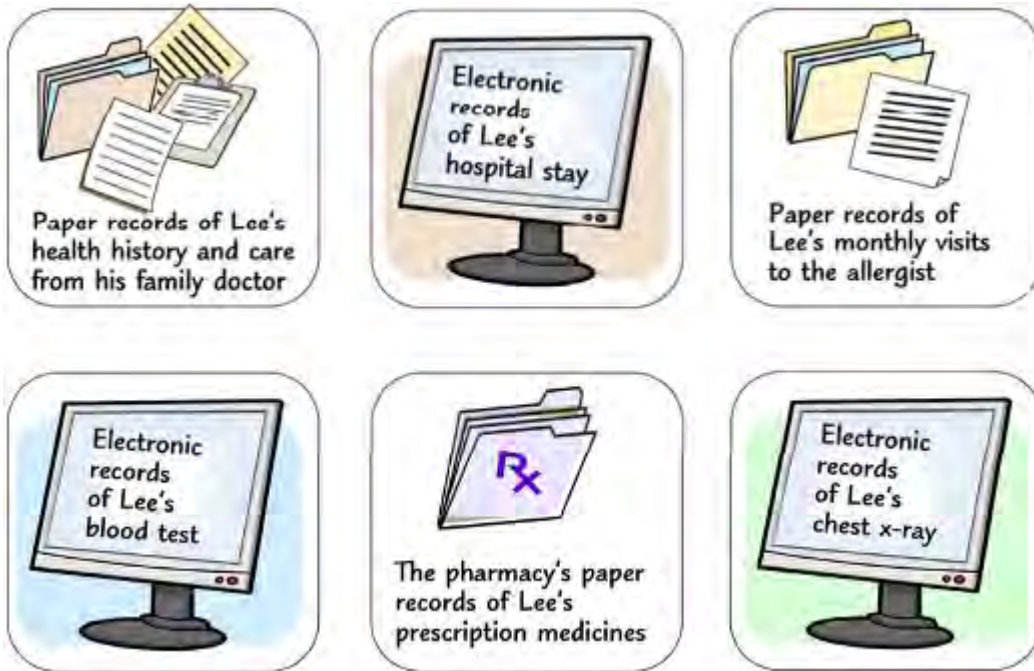
Some medical records are kept in computer files

When your personal health information is kept in a computer file, it's called an “**electronic health record**.”

When doctors, hospitals, pharmacies, and other organizations use electronic health records, they put information about you and your care into a computer instead of putting it into a filing cabinet.

For example, instead of writing notes on a piece of paper, your doctor could use a computer to type notes into your electronic health record.

EXAMPLE for a patient named Lee



How can you tell whether your medical records are being kept in folders or computer files?

It can be hard to know whether your medical records are being kept in folders or computer files. *If you don't know, just ask.*

The Secure Network - what is it for?

When your medical records are kept in different places, it can take time and effort for your doctors to get the information from these records

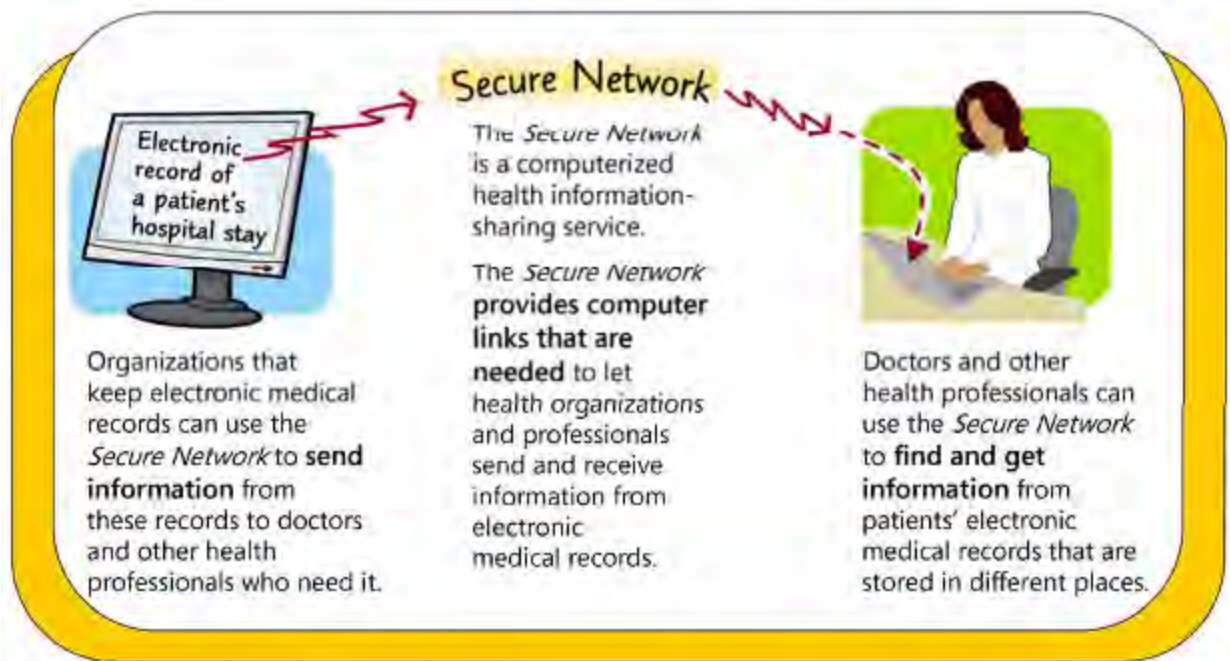
To give you the best possible care, your doctors and other health professionals need information from your medical records that tells about your health history and the care you have already received.


Whether your medical records are stored in filing cabinets or in computer files, it can take some time for your health professionals to get the information from these records.

- If your records are kept in folders at different places, copies can be sent to your health professional by fax or by mail. This takes some time and there can be delays.

- If your records are kept in computer files in different places, it can also be hard for your doctors to get information from these files.
 - f Each place that keeps your medical records in computer files has its own computer system.
 - f Organizations with different computer systems can have trouble communicating with each other.
 - f This means it will be hard for these organizations to share your personal health information from one computer system to the next.
- If it's hard to bring together information from your different medical records, your doctors might see *only part* of your personal health information.
 - f Important information might be missing.
 - f It is possible that no doctor will be aware of your complete health history.

 **The Secure Network brings together information from your electronic medical records that are stored in different places**



 Paper records of health history and medical care **cannot** be sent electronically on the *Secure Network*.

Using the Secure Network can help your doctors and other health professionals give you better care

Using the Secure Network gives health professionals quick and easy access to your electronic medical records

- When they use *Secure Network*, your doctors, nurses, and other health professionals can collect information about you from other places where you have gotten care.
- When your health professionals have more information about you, it can help them give you better care. Here are two examples:
 - f* If you have a medical emergency, quick computer access to your electronic medical records could mean the difference between life and death.
 - f* If you need medical help after regular office hours, the doctor on call can look up your health information on a computer by using the *Secure Network*.

Using the Secure Network encourages teamwork among doctors and others

- By using the *Secure Network*, your doctors and other health care professionals can all get the same information about you.
- When everyone has access to the same information, there's less chance of a mistake or misunderstanding.

Using the Secure Network can help prevent unnecessary care


- Using the *Secure Network* makes it easy for your health professionals to look up records of your previous care. This can keep you from having to repeat tests that have already been done.

The *Secure Network*- an example to show how it works

1

Lee is a patient in the emergency room.

The emergency room doctor uses the *Secure Network* to get information from Lee's electronic medical records that are kept in different places.

- The emergency room doctor has been trained to use the *Secure Network* and has promised in writing to protect the privacy of patient information that he gets by using the *Secure Network*
- To get information about Lee, the emergency room doctor starts by looking at a list that tells what information from Lee's electronic medical records is available by using the *Secure Network*. This list is shown below.
- Then the emergency room doctor marks boxes to tell the *Secure Network* which of Lee's information he wants to see. He wants to see all three pieces of information, so he marks all three boxes (each has a red check mark: .

Report of a heart stress test on July 22, 2006 at Hometown Medical Center (phone number 513-9999)



Report of a hospital stay on December 2-8, 2006, at Riverside Hospital (phone number 513-4444)



Results from a blood test on March 11, 2005 at Jones Medical Laboratory (phone number 513-3333)

Some of Lee's health information was not available by using the *Secure Network* because it was not in a computer file.

- Paper medical records *cannot* be sent by using the *Secure Network*.
- The emergency room doctor could not use the *Secure Network* to get information from any of the following paper medical records of Lee's care:



Records from Lee's family doctor



Records of Lee's prescription medicines



Records of Lee's allergy visits

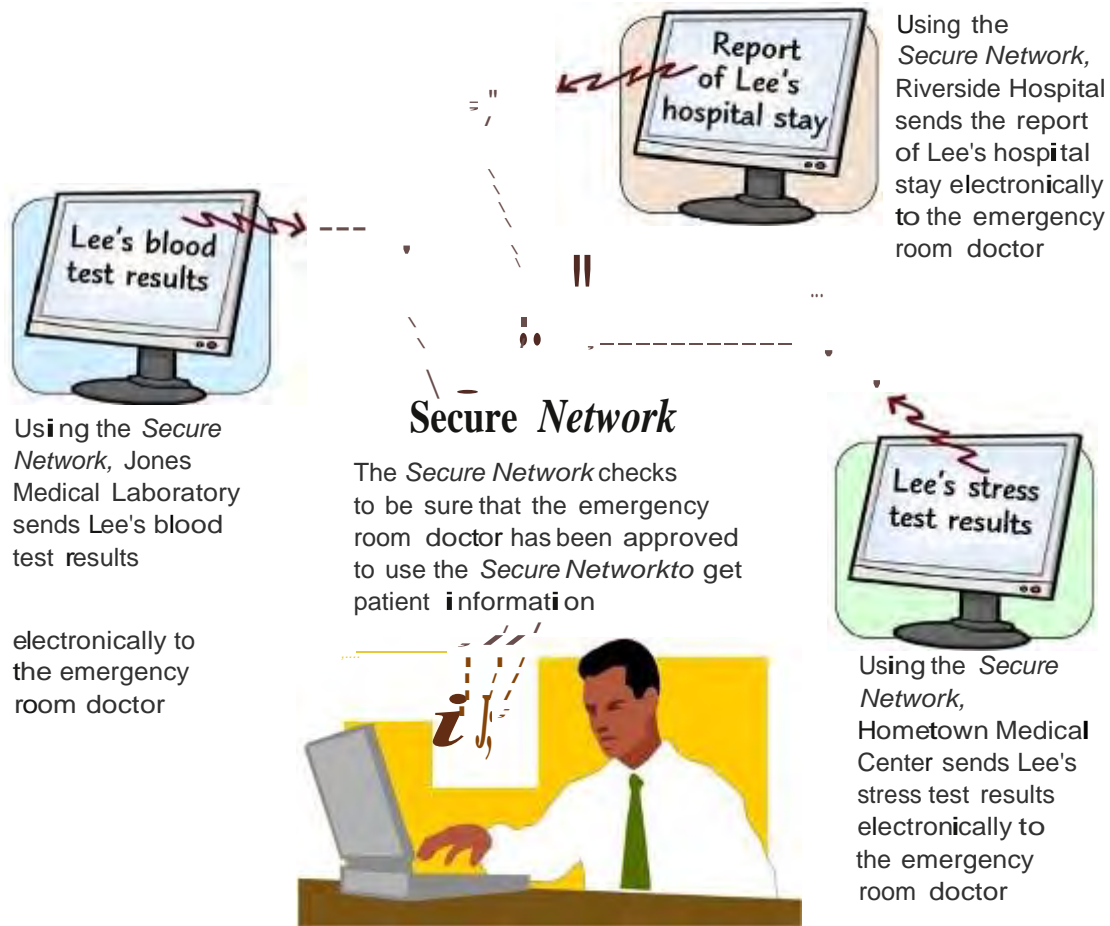
2

The *Secure Network* sends electronic messages to each of the three places where Lee's information is stored. These messages tell them which information about Lee they should send to the emergency room doctor.

- The *Secure Network* is an information sharing service – it's **not** a health information "data bank." This means that the *Secure Network* does not actually store any of Lee's personal health information.
- The information the emergency room doctor wants to see is actually stored at Hometown Medical Center, Riverside Hospital, and Jones Medical Laboratory.
- When the emergency room doctor requests the information about Lee, the *Secure Network* delivers this request to the three places where Lee's information is stored.
- When these places get the request from the *Secure Network*, they send the Lee's information to the emergency room doctor. This happens automatically.

3

The information requested by the emergency room doctor is delivered to him using the *Secure Network*.



4

The emergency room doctor put the information about Lee's hospital stay, blood test, and stress test into the records he made about Lee's visit to the emergency room.

- When they use the *Secure Network* to get information from a patient's electronic medical records, doctors and other health professionals are allowed to put copies of that information into the medical records they keep for that patient.

What kinds of information from your electronic medical records can be shared by using the *Secure Network*?

As of March 2007, the following kinds of information from electronic medical records can be sent and received by using the *Secure Network*:

Reports of hospital stays

- These reports tell what happened during the hospital stay.

Test results

- Test results include results from blood tests, urine tests, and other types of tests done by medical laboratories.

Diagnostic images

- "Diagnostic images" are like pictures of the inside of your body. Examples are x-rays, ultrasounds, mammograms, MRIs, and CT scans.
- The information about diagnostic images that is shared on *Secure Network* includes a report about what the image means. Often the image itself (such as an x-ray) can also be sent electronically using *Secure Network*.

Reports from specialists

Here are two examples:

- A report from a cardiologist (heart specialist) that tells the results from a stress test.
- A report from a pathologist that tells the results for a tissue sample that was tested for cancer.

Prescription medications

- The following information is included for original prescriptions and refills: the name of the medication; the amount of medication; and the date when the patient picked it up at the pharmacy.

You can get an updated list

For an updated list of what kinds of patient information are available by using the *Secure Network*, you can visit the website at www.securenetwork.org. Or you can get the updated list by calling *Secure Network Customer Service* (1-800 123-4567).

Information shared on *Secure Network* covers a three-year period

In general, the patient information that is shared on *Secure Network* is for care provided during the last three years.

You can get a list of organizations and health professionals that use the *Secure Network* to send information from their electronic medical records

- To get this list, call *Secure Network Customer Service* at 1-800-123-4567 or visit the website at www.securenetwork.org
- All organizations and health professionals on this list have been trained to use the *Secure Network*. They have also promised in writing to follow the *Secure Network's* rules for protecting the privacy and security of patients' personal health information that is sent by using *the Secure Network*.

Who can use the Secure Network to see information about you?

Doctors and other health professionals who are providing your care are the only ones allowed to see the information about you

- The *Secure Network* Company does not allow anyone to use the *Secure Network* to sell you things or ask you for money.
- The *Secure Network* Company does not allow anyone to use the *Secure Network* to handle payments for your care.
 - f Organizations such as health insurance companies need certain types of information about your medical care in order to handle payments for your care. They get this information about your medical care in other ways that do not involve using the *Secure Network*.
- *Secure Network* does not allow employers, life insurance companies, drug companies, or other companies to see any information about you that is shared using *Secure Network*.
 - f These organizations may have other ways to see your personal health information that do not involve using the *Secure Network*.

To see information using *Secure Network*, doctors and other health professionals must be trained and must follow certain rules

- All health professionals who use the *Secure Network* must be trained to use it.
- All health professionals who use the *Secure Network* must promise in writing to follow *Secure Network*'s rules for protecting the privacy and security of the patient information that is sent by using the *Secure Network*.

Are you allowed to see the information about you that is being shared on *Secure Network*?

You can see a list that tells what kind of information about you is available by using the *Secure Network* – but you cannot use the *Secure Network* to see the actual information

- If you want to see what is in these records, you can ask the doctors and others who provided your care to show you what is in the medical records they keep about your care.

EXAMPLE

Here is the list of information for a patient named Ed that is available by using the *Secure Network*:

- Prescription medicines** on January 18, 2006, August 22, 2006; and March 3, 2007; at Corner Pharmacy (phone number 513-8888)
- Report of a hospital stay** on October 4-6, 2006, at Eastside Hospital (phone number 513-2222)
- Results from a urine test** on March 11, 2007 at Jones Medical Laboratory (phone number 513-3333)

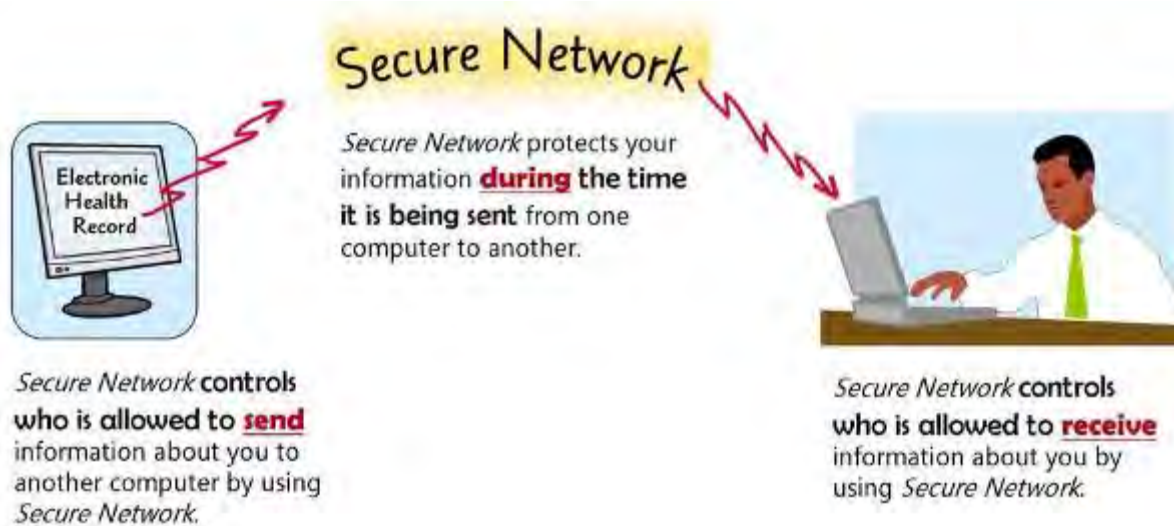
- Ed can see this list that shows types of information, but he cannot use the *Secure Network* to see the actual information that is mentioned in this list.
- This means that Ed cannot use the *Secure Network* to see the list of prescription medicines he got at Corner Pharmacy, or the report of his hospital stay, or the results from his urine test.
- If Ed wants to see any of this information, he will need to ask the pharmacy, hospital, or medical laboratory to show it to him. It's also possible that Ed's family doctor has all of this information and can show it to Ed.



How to find out what kinds of information about you are available to health professionals who use the *Secure Network*

- You can use a computer to visit www.securenetwork.org. On the homepage, click on the link that says "Information for patients."
- Or you can call 1-800-123-4567 and ask *Secure Network Customer Service* to send you a printed copy of the list.

How does the Secure Network protect the privacy and security of your health information?



- ▶ All persons who use Secure Network to send or receive health information are trained to keep patient information private.

 - They must sign a legal agreement that says they will not share any patient information with anyone who does not have permission to see it.
 - Anyone who breaks the *Secure Network's* security rules will be punished.
- ▶ The Secure Network Company keeps track of who uses the Secure Network to look at your personal information

 - When medical information is kept in paper records, there's no easy way for you to know who sees your personal health information.
 - *It's different for electronic record keeping. The Secure Network Company keeps track of who has used the Secure Network to look at your health information.*
 - f These records tell the person's name, their organization, the date, and which pieces of your information the person saw.
 - f For a copy of these records, please call *Secure Network* Customer Service at 1-800-123-4567.

There are several layers of very strict security safeguards

- *Secure Network's* computer system watches for signs of suspicious activity. The system has alarms to warn us about possible security problems so that we can check on them.
- If there is ever a security problem that affects your personal information, we will let you know. This includes, for example, telling you if we discover that any of your information has been stolen, lost, tampered with, or seen by people who should not be allowed to see it.

To safeguard the security of the electronic system, there are backup copies

- To guard against possible loss or damage from fire, earthquake, or other disaster, there are backup electronic copies of the records about who has used the *Secure Network* to look at your personal health information.
- The *Secure Network* does *not* keep copies (or back-up copies) of your personal health information.

Your information will be shared on the *Secure Network* unless you "**block**" the sharing

What does it mean to "**block**" the sharing of your health information on the *Secure Network*?

"Blocking" means that you are "**turning off**" the **sharing** of your personal health information on the *Secure Network*.

"Blocking" your information means that **no one will be allowed to see the information about you** by using the *Secure Network*.

The *Secure Network Company* **assumes** that **you agree** to have your information shared electronically on *Secure Network* -- unless you say "no"

- If you are okay with having information from your medical records shared electronically using *Secure Network*, you do not need to do anything. The *Secure Network Company* will keep on allowing your information to be shared on the *Secure Network*.

- If you are not okay with having information from your medical records shared electronically using *Secure Network*, you must follow the instructions below that tell how to block your information.



Asking Secure Network to block your information does not block any other ways of sharing your personal health information

The Secure Network is only one way in which a patient's personal health information is shared from one organization to another. There are many other ways of sharing information that have nothing to do with *Secure Network*.

Here are examples of information sharing that **do not involve** using the *Secure Network*:

- Laws require that some types of personal health information be reported without getting the patient's permission. Examples include: reporting when a baby is born; reporting some types of diseases that can spread to other people; reporting gunshot wounds and suspicious injuries to the police; and providing health information if a judge gives the order.
- There are organizations that check on quality of care by looking at medical records kept by doctors, hospitals, clinics, nursing homes, and other health care providers. Some of your personal health information might be seen by these organizations. They follow strict standards to safeguard your privacy.
- To handle payments for your care, organizations such as health insurance companies and health plans need to get certain information about the care you have received.

How to block all sharing of your personal health information on the Secure Network



If you do not want any of your information to be shared using *Secure Network*, you must tell the *Secure Network Company* to block all sharing of your information

- If you block all sharing of your information, none of your doctors or other health professionals will be able to use the *Secure Network* to get information about you – even if you are having a medical emergency.
- If you block all sharing of your information, the *Secure Network* will stop letting people use *Secure Network* to see information about you.

However, your information can still be shared in many other ways by many other organizations besides *Secure Network*.

- Asking the *Secure Network Company* to block your information does not change anything in your medical records. The doctors and other health professionals you see will continue to keep their own records about your care just as usual.



How to block all sharing of your information on the Secure Network:

- To block the sharing of your information, you must contact *Secure Network Customer Service*. The phone number is 1-800-123-4567. If you call from anywhere in Oregon, this call is free. Or you can use a computer to visit the website at www.securenetwork.org. Click on the link that says “Request to block sharing of my health information on *Secure Network*.”
- The *Secure Network Company* will send you a letter that tells when blocking will begin. This letter will also explain the rules that apply to blocking your information.



If you block the electronic sharing of your information on Secure Network, you can change your mind and have it “unblocked”

- To “unblock” your information, call *Secure Network Customer Service* at 1-800-123-4567 or visit the website at www.securenetwork.org.

How to block only part of your information from being shared on the Secure Network



To stop only part of your information from being shared on the Secure Network, you must contact the place that is sending this piece of information to be shared on Secure Network and tell this place to stop sending it.

- For example, if the piece of information you want to block is a hospital report, you would contact the hospital and ask them to stop sending this report to be shared on *Secure Network*.
- On the next page, there is an example that shows more about how to block certain parts of information from being shared on *Secure Network*.

Here's an example about a patient named Anna:



Anna is using her computer to find out what information from her medical records can be seen by people who are using *Secure Network*.

She finds a list.

(If Anna didn't have a computer, she could call *Secure Network* and get this same list.)

The list is shown below. It includes three pieces of information from her medical records and each piece is from a different place.

The list of information about Anna:

Report from a hospital stay on June 22-24, 2005, at Community Memorial Hospital (phone number 234-2222)

Report of a chest x-ray on October 18, 2006 at Westside Medical Center (phone number 234-1111)

Results from a blood test on January 20, 2006 at Smithville Medical Laboratory (phone number 234-5555)

Anna decides that she does not want these blood test results to be seen by anyone who is using *Secure Network*.

(Anna wants people who are using *Secure Network* to see the reports of her hospital stay and chest x-ray. She only wants to stop them from seeing her blood test results.)

To stop people from seeing her blood test results, Anna must tell the place that has the records of her blood test results to stop sending these results to *Secure Network*.

The list tells Anna that her blood test results come from Smithville Medical Laboratory. It gives the phone number for this laboratory.



Anna calls Smithville Medical Laboratory.

She tells the lab to stop sending her blood test results to people who are using *Secure Network*.

Final testing version

(please inform and acknowledge the source if you use this material)

How to contact the Secure Network Company if you have questions or want to make a complaint

How to contact the Secure Network Company

- You can call the *Secure Network Customer Service* at 1-800-123-4567 (this phone call is free).
- Or you can use a computer to connect to the website at www.securenetwork.com and click on the link that says “customer service.”

Secure Network Customer Service will get back to you within two days (not counting weekends or holidays).

- If you have questions, *Customer Service* will give you answers.
- If you have a complaint, *Customer Service* will let you know what is being done to take care of your complaint.

APPENDIX D

“Personal Electronic Health Record” explanatory sheets

This appendix shows the explanatory materials used in Part 2 of the consumer interviews



What is a "Personal Electronic Health Record"?

Having a *Personal Electronic Health Record* is like having your own **"personal bank account" for health information.**

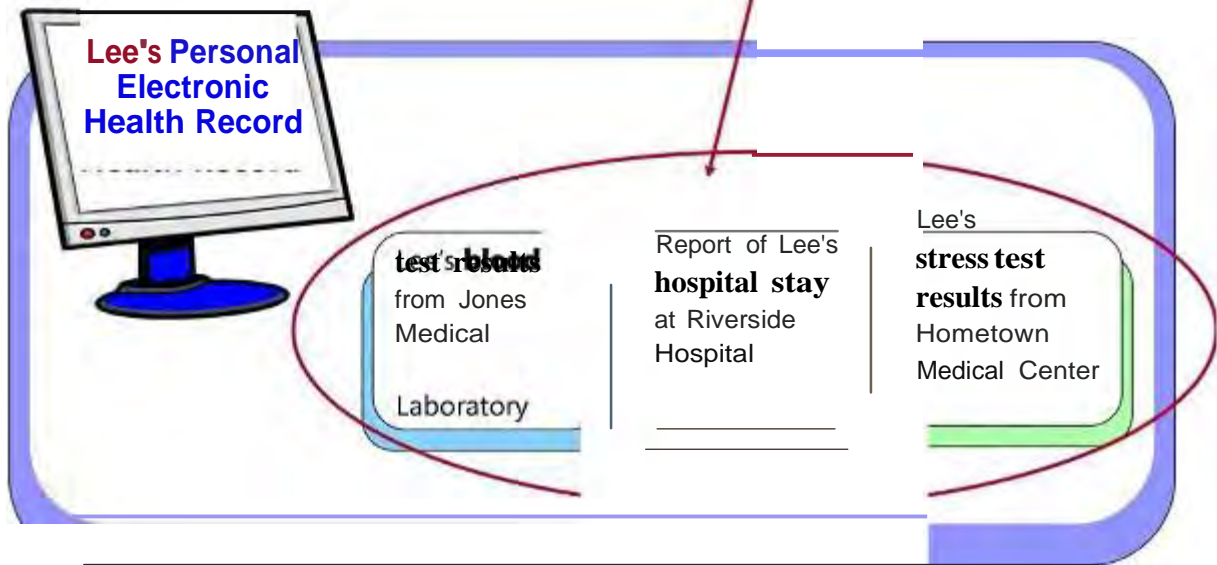
A *Personal Electronic Health Record* puts your information together **in one place.**

You are the one who "owns" and manages this personal health record:

- The information for your personal health record is brought in electronically from various places where your medical records are stored. This information is updated automatically.
- You can see of the information in your medical records.
- You decide which information from your medical records should be included in your personal health record. If you want to, you can remove certain information.
- You can also add your own health-related information to your personal health record. For example, you could add information about your family health history or about which people should be contacted if you have a medical emergency.
- You can add notes and comments to your personal health record, such as adding comments on some of the health information it contains
- You decide who can see your personal health record and which parts they can see.
- It's quick and easy for you to keep track of who looks at your personal record and which parts they look at.
- If you make additions or changes to your personal record, they are effective right away.

EXAMPLE Lee has a *Personal Electronic Health Record*

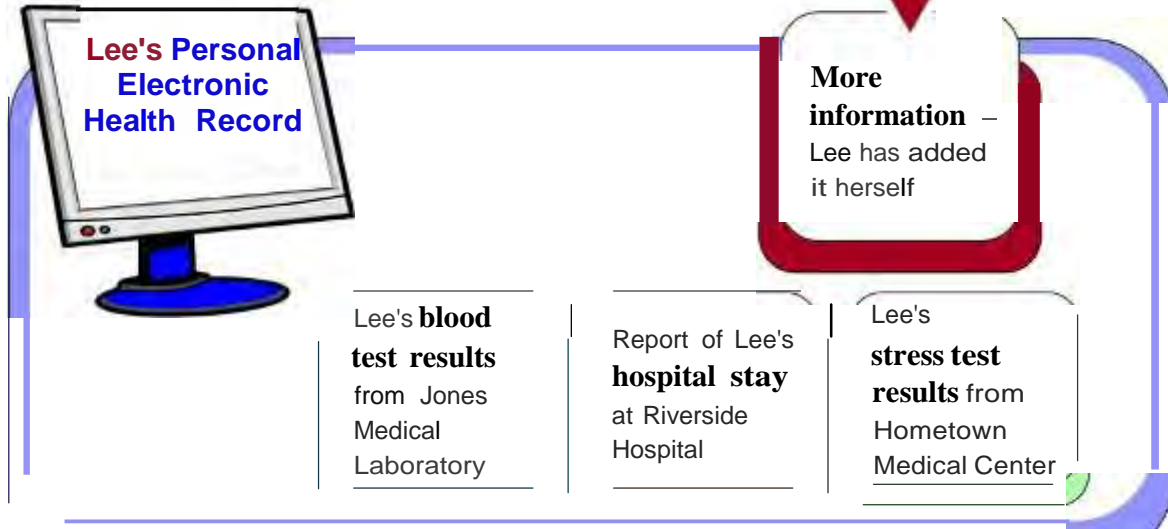
Lee's personal health record includes the same three pieces of information about Lee that the emergency room doctor got by using the *Secure Network*.

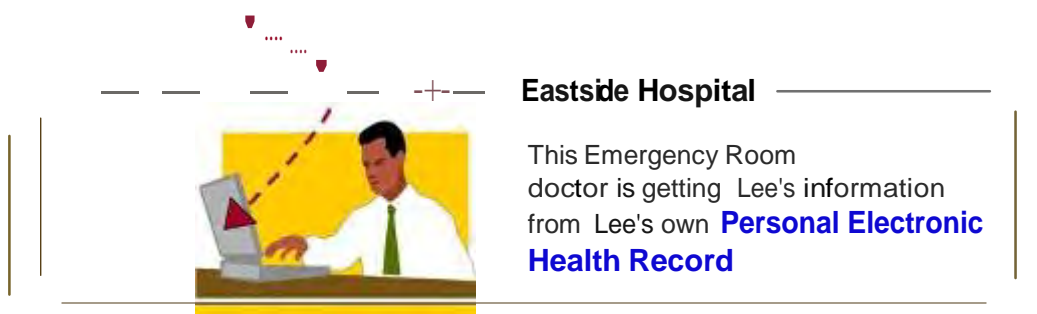
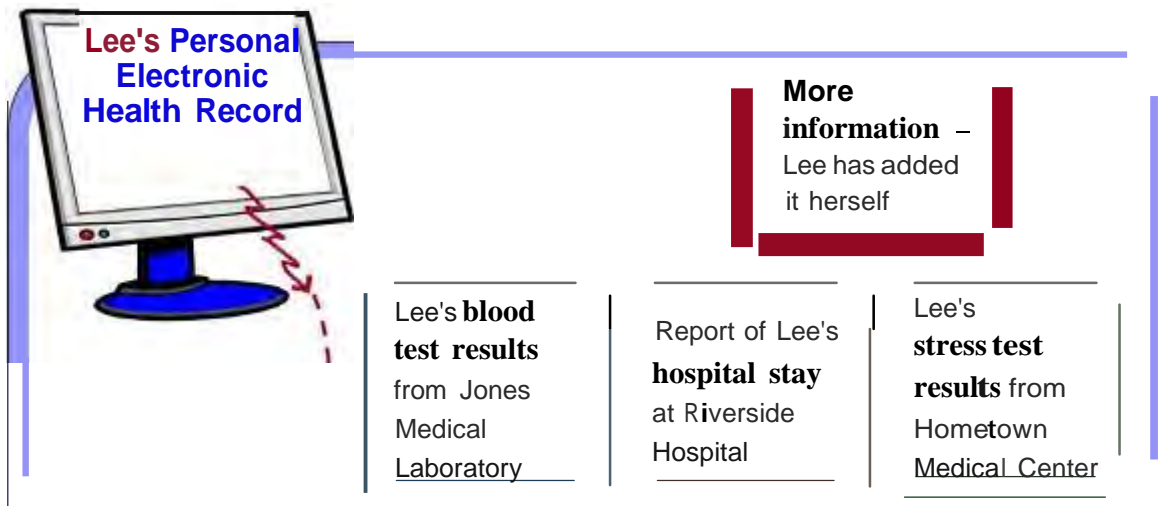


Lee can add information to her *Personal Electronic Health Record-*

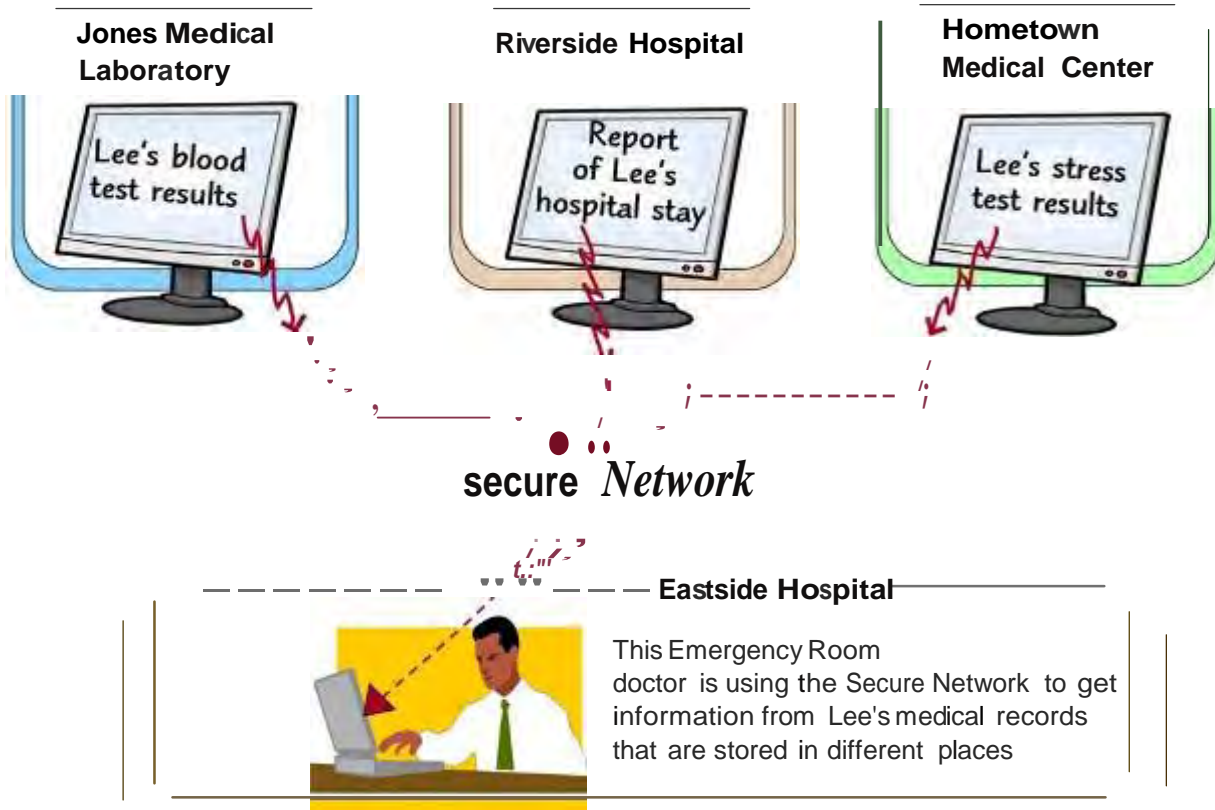


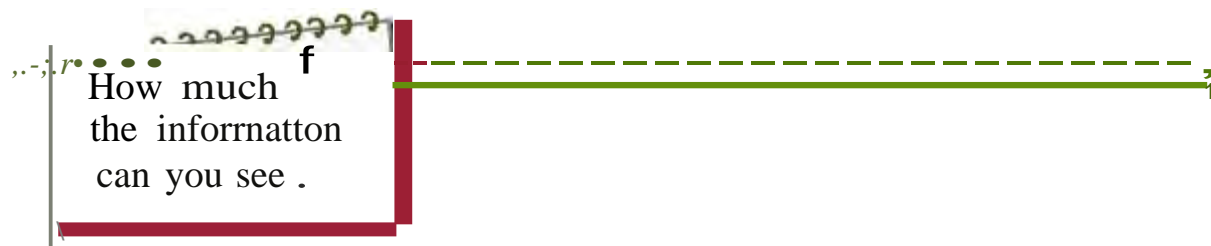
- Information about her family health history, vaccinations, immunizations, and allergies to medications
- Name and contact information for her family doctor
- Who to call in an emergency





Using the *Secure Network* to get Lee's health information from **three different places**:





secure Network

You can only see a list that shows what *types* of information

- You can get a list that tells which pieces of information from your electronic medical records are available to the health professionals who use the *Secure Network* to get your health information.
- You cannot use the *Secure Network* yourself to see the actual information from your medical records.
- (If you want to see the actual information in your medical records, you have to ask the doctors, hospitals, and other places to show it to you.)



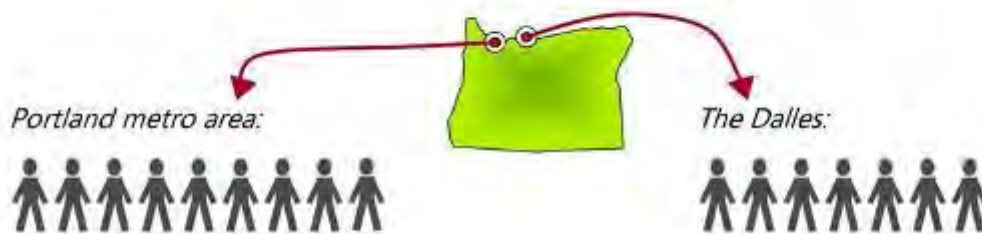
You can see all of the information

- Having a *Personal Electronic Health Record* is like having your own "personal bank account" for health information.
- You "own" and manage your *Personal Electronic Health Record*.
- You can see everything that is in your own *Personal Electronic Health Record* (You are the one who decides what information to include in it.)

APPENDIX E

Profile of the 16 consumers who were interviewed

The 16 interviews were done in two Oregon locations:



A mix of women and men:



Ranging in age from 25 to 75:



Nine with a high school education; seven with up to four years of college



Nearly all have looked for health information on the internet:

Has looked for health information on the internet



Has not looked for health information on the internet



Most have a chronic health care condition

Has a chronic health condition



Does not have a chronic health condition



How many doctor visits in the last 12 months?

1-2 visits



3-5 visits



6-9 visits



10-15 visits



16 or more



How many ER visits in the last 12 months?

None



One or more



How many hospital stays in the last 3 years?

None



One or more

