

PRIVACY AND SECURITY BARRIERS TO THE ELECTRONIC EXCHANGE OF HEALTH INFORMATION

A Minnesota Privacy and Security Project Report for the:

Privacy and Security Solutions for Interoperable Health Information Exchange Contract

Submitted by:

James I. Golden, Project Director
Minnesota Privacy and Security Project
Minnesota Department of Health
85 East Seventh Place, Suite 220
Saint Paul, MN 55101

On Behalf of:

The Minnesota e-Health Advisory Committee

Submitted to:

Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange

Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

November 3, 2006



The Minnesota Privacy and Security Project expresses its gratitude for the assistance, time, and effort of the individuals and organizations that participated in the Project's Work Groups and ad-hoc meetings. These participants' input and analysis has been critical to accomplishing the goals of the project and in identifying and documenting the privacy and security barriers identified in this report.

**Questions or comments regarding
this report should be directed to:**

The Minnesota Privacy and Security Project

James I. Golden, Project Director
Minnesota Privacy and Security Project
Minnesota Department of Health
85 East Seventh Place, Suite 220
Saint Paul, MN 55101

E-mail: james.golden@health.state.mn.us
Telephone: 651.201.4819



TABLE OF CONTENTS

Table of Contents	1
Fact Sheet	2
Executive Summary	3
Privacy and Security Barriers to the Electronic Exchange of Health Information	4
Background and Purpose	8
The Minnesota e-Health Initiative	8
The Minnesota Privacy and Security Project	9
Health Information Exchange - Concepts and Terminology	10
Project Methodology	12
Project Structure	12
Project Activities	14
Privacy and Security Barriers to the Electronic Exchange of Health Information	16
Introduction	16
Consumer Trust and Acceptance of Health Information Exchanges	17
Minnesota’s Patient Consent Requirements - General	19
Impact of Minnesota’s Patient Consent Requirements on Locating Patients’ Health Information.....	20
Impact of Minnesota’s Patient Consent Requirements on the Exchange Patients’ Health Information...	24
Operational Difficulties in Implementing Electronic Access to Patient Information.....	31
Liability Concerns as a Barrier to the Exchange of Health Information	37
Conclusions.....	38
Table of Contents for Appendices	40
Appendix A Variations and Legal Work Group Members	44
Appendix B Nine Domains of Privacy and Security	47
Appendix C 18 Health Information Exchange Scenarios	48
Appendix D Summary Findings	
Analysis of 18 Health Information Exchange Scenarios	85

FACT SHEET

Under the Minnesota e-Health Advisory Committee's direction, the Minnesota Privacy and Security Project has conducted a systematic review of current laws and practices to identify the most significant privacy and security issues facing organizations in implementing the electronic exchange of health information.

Health industry stakeholder and consumer involvement are critical to ensuring that the project's results are broadly acceptable and applicable to the community and this report's information has been gathered from interested stakeholders and consumer representatives over 12 meetings and 30+ hours of discussion and analysis.

The original premise of the project was that significant variations across organizations' business practices for handling and disclosing health information are a significant barrier to exchanging data. However, the project found that organizational variation was not a significant barrier to the exchange of health information.

The project revealed that the real privacy and security issues impeding the electronic exchange of health information are universal, overarching issues that impact all types of health care organizations and apply to all types of health information. Many of these privacy and security issues arise not because organizations have different practices around the issues. Rather, they are an impediment because organizations have not found any fully adequate mechanisms to address the issues.

The overarching privacy and security issues that must be solved to advance the appropriate electronic exchange of health information are:

- **Implementation of Minnesota's patient consent requirements within a health information exchange;**
- **Operational difficulties in first providing, and then limiting and monitoring external organizations' electronic access to patient data; and**
- **Liability concerns with the inappropriate disclosure of patients' health information.**

The privacy and security barriers to the electronic exchange of health information identified in this report are a mix of legal, technological, and organizational issues that need to be addressed through a variety of means. The actions necessary to address the barriers to advancing the electronic exchange of health information can be summarized as:

- **Patient consent requirements must be clarified;**
- **Technology must be developed and organizational policies changed to address operational difficulties in providing, limiting and monitoring external organizations' access to patient data; and**
- **A legal, technological and organizational framework must be developed to address organizations' liability concerns that are operationally feasible for ensuring the privacy, security, and confidentiality of patients' data.**

These barriers may be difficult to reduce or eliminate. However, prioritizing action around these privacy and security issues is necessary to facilitate development and implementation of health information exchanges. Finding workable solutions to these barriers will improve the privacy and confidentiality of patients' data and reduce the liability concerns that impede health care organizations' willingness to engage in the electronic exchange of information.

EXECUTIVE SUMMARY

In 2005, the Governor and the Minnesota Legislature made e-Health a state priority by establishing the Health Information Technology and Infrastructure Advisory Committee (aka, Minnesota e-Health Advisory Committee¹) in Minnesota Statutes § 62J.495. The Minnesota e-Health Advisory Committee is charged with advising the Commissioner of Health on health information technology issues and goals. One of the committee's responsibilities is to address the critical issues of security and confidentiality of health information and patient privacy requirements in this new era of electronic health information exchange. This report is a first step in fulfilling that responsibility.

Under the Minnesota e-Health Advisory Committee's direction, the Minnesota Privacy and Security Project (MPSP) has conducted a systematic and comprehensive review of current laws and practices to identify the most significant privacy and security issues facing organizations in implementing the electronic exchange of health information. Specifically, the project is intended to:

- Identify the most significant privacy and security barriers impeding the appropriate electronic exchange of health information;
- Document how privacy and security concerns impede the exchange of health information;
- Describe the causes and rationale for the privacy and security barriers; and
- Develop solutions and implementation plans to eliminate or reduce privacy and security barriers to the exchange of health information, while maintaining or strengthening privacy protections afforded to patients' health data.

This report completes the first three tasks and work to complete the fourth is about to begin.

The MPSP was launched with Minnesota's award of a \$350,000 Health Information Security and Privacy Collaboration (HISPC) contract to examine privacy and security issues related to health information exchanges. The HISPC contract is part of a U.S. Department of Health and Human Services' project titled, "*Privacy and Security Solutions for Interoperable Health Information Exchange*".²

Health industry stakeholder and consumer involvement in this project are critical to ensuring that the MPSP's results are broadly acceptable and applicable to the community. The MPSP is structured to provide all interested individuals the ability to participate directly and follow the project activities through our website³. The information for this report has been gathered over 12 meetings and 30+ hours of discussion and analysis in two work groups:

- **Variations Work Group** – This work group consisted of privacy and security experts representing health systems, health plans, hospitals, public health agencies, local units of government, and other organizations involved in the exchange of health information.
- **Legal Work Group** – This work group consisted of legal experts representing consumers, health systems, health plans, hospitals, public health agencies, and other organizations involved in the exchange of health information.

¹ More information on the Minnesota e-Health Advisory Committee's activities can be found at:
<http://health.state.mn.us/e-health>

² Contract #290-05-0015 from the Agency for Healthcare Research and Quality

³ <http://health.state.mn.us/e-health/mpsp/>

This report represents the synthesis of the two work groups' activities, which included:

- Analyzing HISPC situational-based scenarios, which investigated organizations' policies, practices, and mechanisms for exchanging health information;
- Discussing privacy and security issues identified by organizations as part of their internal implementation of electronic health records;
- Describing privacy and security issues encountered when organizations have attempted to electronically exchange health information with other organizations;
- Examining current and emerging models of health information exchanges and identifying privacy and security concerns related to the exchange of information in these models; and
- An in-depth investigation of organizations' interpretation and implementation of Minnesota's patient consent requirements.

PRIVACY AND SECURITY BARRIERS TO THE ELECTRONIC EXCHANGE OF HEALTH INFORMATION

The original premise of the project was that significant variations across organizations' business practices for handling and disclosing health information are a significant barrier to exchanging data. However, the premise was not supported by the work groups' analyses. In general, and with the notable exception of patient consent, the project did not find significant variations in business practices across organizations. Indeed, most organizational variation identified was not deemed a significant impediment to the appropriate exchange of health information.

The MPSP revealed that the real privacy and security issues impeding the electronic exchange of health information are universal, overarching issues that impact all types of health care organizations and apply to all types of health information. Throughout all of the project's activities, a select set of issues were repeatedly identified as major privacy and security concerns that represent serious impediments to advancing the electronic exchange of health information. Many of these privacy and security issues arise not because organizations have different practices around the issues. Rather, they are an impediment because organizations have not found any fully adequate mechanisms to address the issues.

The overarching privacy and security issues that must be solved to advance the appropriate electronic exchange of health information can be grouped into three general issues:

1. **The implementation of Minnesota's patient consent requirements within a health information exchange.** This issue has two parts. First, there are significant and irreconcilable differences in organizations' interpretations of Minnesota's patient consent requirements. These differences make it impossible for health care providers to agree on "when" and "how" patient consent is required. Second, the patient consent requirements were designed for paper-based exchanges of information and early electronic data base systems are not conducive to a real-time, automated electronic exchange of information.
2. **Operational difficulties in first providing, and then limiting and monitoring external organizations' electronic access to patient data.** This issue is identified as one general issue, because it is a set of interconnected security problems that must be addressed concurrently to successfully implement a health information exchange. To give external health care providers appropriate access to electronic health records and patient data, organizations need to address four security topics, for which there are fully adequate solutions:

- a. Mechanisms to establish and maintain a list of individuals authorized to access patient data;
 - b. Methods to authenticate authorized individuals who access patient data;
 - c. Information access controls – within information systems and through coordinated organizational policies – to limit authorized individuals' access to the patient data that is appropriate for the individual's functions and needs; and
 - d. Mechanisms for coordinated auditing across organizations to identify authorized individuals who inappropriately access health information.
3. **Liability concerns with the inappropriate disclosure of patients' health information.** Health care organizations face liability from various sources for the inappropriate disclosure of patient data. Consequently, health care organizations are very conservative in their approach to exchanging data. Health care organizations explicitly consider organizational risk as a factor in their decision to participate in a health information exchange. That is, they want to be confident that the health information exchange has appropriately addressed privacy/security issues to minimize their organization's liability from inappropriate disclosures of patients' data.

Within each of the general privacy and security issues there are a number of specific issues that need to be addressed to advance electronic exchange of health information while maintaining or strengthening patient privacy protections. The following list provides a summary description of the privacy and security barriers uncovered through the project:

Minnesota's Patient Consent Requirement

The term "Health Records" is not defined in Minnesota Statutes § 144.335. There is disagreement about whether or not patient's demographic data and a pointer to the location of patient's health information is a "health record." Consequently, there is disagreement about "when" and "how" patient consent is required in mechanisms to assist health care providers in locating their patients' health information. Identifying the locations of patients' health information is a necessary first step to exchanging information.

The term "Current Treatment" is not defined in Minnesota Statutes § 144.335. There are at least two interpretations for the term "current treatment" as used in Minnesota's patient consent requirements, which results in substantially different interpretations of "when" patient consent is needed and "how" it should be obtained. The wide spectrum covered by the interpretations means Minnesota does not have a uniform foundation on which to build its information exchanges. This lack of a common foundation will complicate and delay the development of electronic exchange and create variability in patient privacy protections.

The term "Medical Emergency" is not defined in Minnesota Statutes § 144.335. Prior to releasing a patient's health information without consent during an emergency, a health care provider generally needs to make some assessment that the patient is in a medical emergency and unable to provide consent. When the releasing provider and the treating provider disagree about the emergency nature of the patient's situation, they will also disagree about the need for patient consent to release health information.

The term "Related Health Care Entities" is not defined in Minnesota Statutes § 144.335. Patient consent is not required to disclose patients' health information within "related health care entities." However, the inability for providers to clearly agree on the definition of "related health care entities," means that they also cannot agree on when patient consent is required for the release of patients' health information.

Minnesota's patient consent requirements place all responsibility and liability for the appropriate release of patients' health information on the health care provider releasing information and place no responsibility on health care providers requesting the information. To protect their

patients' privacy and to minimize their liability, health care providers have developed and implemented many policies and practices associated with obtaining, documenting, and validating patient consent for the release of health information. Many organizations' policies and procedures were developed to reduce liability concerns rather than to facilitate the rapid exchange of information. Consequently, most patient consent policies and practices require extensive human activity, oversight, and involvement and are unable to facilitate the real-time, automated exchange of patients' health information.

Additionally, Minnesota law does not provide a framework or mechanism to transfer/share current responsibilities and liability from the disclosing provider to the requesting provider, even though it is the requesting provider that:

- Is most likely to have a current treatment relationship with the patient;
- Is most likely to have face-to-face interaction with the patient and the ability to address consent-related issues; and
- Is in the best position to help the patient understand what information is needed, why it is needed, the consequences of not having the information, and the consent required to obtain the information.

Operational Difficulties in Implementing Electronic Access to Patient Information

Organizations have difficulty creating mechanisms to establish and maintain a list of individuals authorized to access patient data. The first issue facing organizations in a health information exchange is determining who should be authorized to access their organization's electronic health records. The task of managing the list of authorized individuals across organizations is difficult as the organizations' staff changes. Organizations need mechanisms to quickly exchange information between their human resource departments and mechanisms to use the information to add and remove authorized users in a timely fashion. This task becomes increasingly difficult as the number of organizations and authorized individuals increases.

Methods to authenticate authorized individuals accessing patient data are cumbersome and place a burden on health care providers. The second issue facing organizations in a health information exchange is how authorized, external users will be authenticated when accessing health records. Current authentication methods (e.g., passwords and security fobs) create a secure system. However, the system can be cumbersome to use, because individuals may have multiple user IDs and passwords that change frequently. As the number of organizations allowing health care providers access to their electronic health record increases, so does the number of user IDs, passwords, and security fobs. The need to manage these security measures places a burden on the individual health care provider that acts as a barrier to accessing patient information.

Organizations are unable to set information system access controls and must rely on coordinated access control policies to appropriately limit authorized individuals' access to patient data. The third issue facing organizations in a health information exchange is how to set access controls to appropriately restrict authorized individuals' access to patient data. Limitations in information systems require organizations to control access through organizational policies. However, achieving compliance with the policies requires organizations to have a coordinated approach to activities that have traditionally not been synchronized across different organizations. At a minimum, organizations need a common approach to:

- Conducting training programs that assist employees in understanding and applying the policies;
- Deploying mechanisms to monitor and audit employees' compliance with the policies; and
- Setting sanctions for disciplining employees who violate the policies.

Organizations need mechanisms for coordinated auditing across organizations to identify authorized individuals inappropriately accessing health information. Auditing individuals' access to patients' health information is critical to protecting the privacy and confidentiality of health information. Organizations generally do not have intelligent tools capable of automatically collecting, organizing, and analyzing the information necessary to assess the appropriateness of individuals' access to health information. The process of collecting and analyzing these data is still a manual, resource-intensive activity.

When an external individual accesses an organization's electronic health records, the organization does not usually have the information necessary to determine if the access is legitimate and must rely on others within the health information exchange to provide information so that the determination can be made. Therefore, significant collaboration and coordination must occur between organizations in a health information exchange for auditing to be effective in protecting the privacy and confidentiality of health information.

Liability Concerns

When health care organizations have liability concerns about the exchange of information, the exchange will generally not occur. Health care organizations face liability from various sources for the inappropriate disclosure of patient data, and therefore are very conservative in their approach to exchanging data. They want to be confident that any mechanism for exchanging health information has adequately addressed privacy/security issues and minimizes their organization's liability. Organizations unable to minimize their liability will not exchange health information. Fear of legal liability is a critical, overarching issue that explains why the most significant barriers are those issues for which organizations have not been able to find any sufficient mechanisms to address privacy and security concerns.

Conclusions

The privacy and security barriers to the electronic exchange of health information identified in this report are a mix of legal, technological, and organizational issues that need to be addressed through a variety of means. The workgroup's analysis of the barriers to be addressed to encourage the electronic exchange of health information can be summarized as follows:

- Patient consent requirements must be clarified.
- Technology must be developed and organizational policies changed to address difficulties in providing, limiting and monitoring external organizations' access to patient data.
- A legal, technological and organizational framework must be developed to address organizations' liability concerns that are operationally feasible for ensuring the privacy, security, and confidentiality of patients' data.

These barriers may be difficult to reduce or eliminate. However, prioritizing action around these privacy and security issues is necessary to facilitate development and implementation of health information exchanges. Finding workable solutions to these barriers will improve the privacy and confidentiality of patients' data and reduce the liability concerns that impede health care organizations' willingness to engage in the electronic exchange of information.

BACKGROUND AND PURPOSE

THE MINNESOTA E-HEALTH INITIATIVE

Introduction

Evidence shows that achieving the full use of health information technology including interoperable electronic health records is critical to improving and ensuring patient safety and quality of health care. In Minnesota, we have committed to ambitious goals to advance the health care industry's use of information technology. A key element to achieving these goals is the ability to efficiently and electronically exchange health information between health care organizations while maintaining appropriate patient privacy protections.

The Minnesota e-Health Initiative

In 2004, the Minnesota e-Health Initiative (MN e-Health) was established as a private–public collaboration to accelerate the use of health information technology in Minnesota. The initiative began with the formation of a statewide committee to advise the Commissioner of Health on health information technology issues and goals. In 2005, the Governor and the Minnesota Legislature further made e-Health a state priority by establishing the Health Information Technology and Infrastructure Advisory Committee (aka, Minnesota e-Health Advisory Committee) in Minnesota Statutes § 62J.495. The Minnesota e-Health Advisory Committee has 26 members who represent key stakeholders including an array of health care providers, payers, public health professionals, and consumers.

The Minnesota e-Health Advisory Committee is responsible for making recommendations to implement a statewide interoperable health information infrastructure, including estimates of necessary resources and standards for: administrative data exchange, clinical support programs, patient privacy requirements, and maintenance of the security and confidentiality of patient data. The investigation of privacy and security issues was identified as a priority project, reflecting the fact that Americans are increasingly worried about the privacy of their health information⁴. The prioritization also reflects:

- The need for health care organizations to deploy common privacy/security policies and technologies that will facilitate the appropriate electronic exchange of health information and ensure uniform, consistent levels of protection for patients' health data across all organizations;
- The need to examine current laws and organizational practices, which have often been developed for a paper-based exchange of data or for early electronic data bases, to identify privacy/security issues and barriers that need to be addressed to enable and facilitate real-time electronic exchange of health information; and
- The desire to identify opportunities for improved privacy protections that provide patients and consumers enhanced access to and control over their health information.

⁴ A more in depth review of patient/consumer concerns regarding the privacy of health information can be found in the Markle Foundation's *The Connecting for Health Common Framework*. The material may be viewed at: <http://www.connectingforhealth.org/>



THE MINNESOTA PRIVACY AND SECURITY PROJECT

Under the Minnesota e-Health Advisory Committee's direction, the Minnesota Privacy and Security Project (MPSP) conducted a systematic and comprehensive review of current laws and practices that both enable and impede the efficient, electronic exchange of health data. The project analyzes the most significant privacy and security issues facing organizations in implementing the electronic exchange of health information in order to:

- Identify the most significant barriers impeding the electronic exchange of health information;
- Document how concerns impede the exchange of health information;
- Describe the causes and rationale for the barriers; and
- Develop solutions and implementation plans to eliminate or reduce these concerns and barriers to the exchange of health information, while maintaining or strengthening privacy protections afforded patients' health data.

To ensure that the MPSP is consistent with other national efforts to examine privacy and security issues related to health information exchanges, the Minnesota e-Health Advisory Committee and Minnesota Department of Health applied for and received a \$350,000 Health Information Security and Privacy Collaboration (HISPC) contract. The HISPC contract is part of a national project from the U.S. Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) and the Agency for Healthcare Research and Quality (AHRQ) titled, "*Privacy and Security Solutions for Interoperable Health Information Exchange.*" The national project, under the direction of RTI International, funds 34 states and territories through HISPC contracts to:

- Assess variations in organization-level business policies and state laws that affect health information exchange;
- Identify and propose practical solutions, while preserving the privacy and security requirements in applicable federal and state law; and
- Develop detailed plans to implement solutions.

Hence, the MPSP has two complementary purposes - to meet the informational needs of the Minnesota e-Health Advisory Committee and to contribute to the national privacy and security agenda by participating in the activities of the HISPC contract.

Minnesota has multiple health information exchange initiatives underway that are reaching various levels of maturity, so it is imperative that our state laws and business practices are understood and harmonized in a way that advances the ongoing development of health information exchanges. Similarly, Minnesota also has a strong culture of respect for individual privacy that is reflected in laws and business practices that are more stringent and protective than the HIPAA Privacy regulations and that need to be integrated into the implementation of health information exchanges. Yet to be truly beneficial, Minnesota must ensure that its efforts around health information exchange and privacy/security issues contribute to and learn from national efforts.

Consequently, the body of this report describes the most significant privacy/security issues to be addressed to advance the development and use of interoperable health information technology in Minnesota. The appendices of the report contribute to the national effort by providing information consistent with the standardized approach prescribed by ONC and ARHQ under the direction of RTI International.

HEALTH INFORMATION EXCHANGE - CONCEPTS AND TERMINOLOGY

This section defines and clarifies a number of terms and phrases used throughout the project to be clear and to assist the reader in understanding the report.

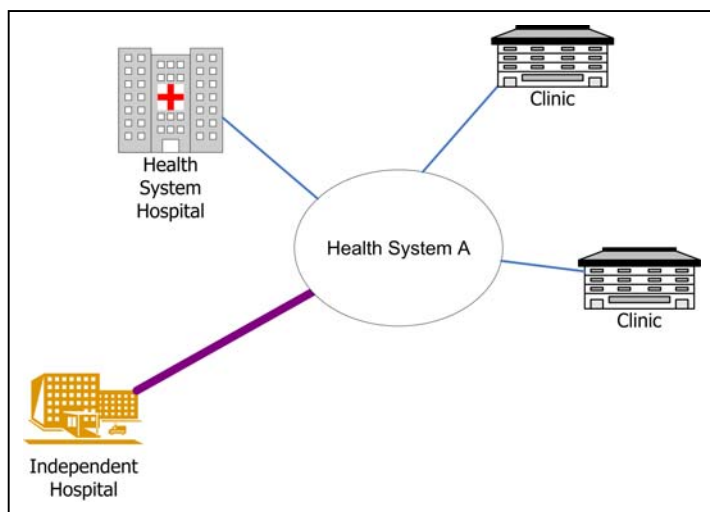
The term **“Health Information”** follows the HIPAA definition and means information related to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Throughout all project materials, the term **“health information” is used synonymously with the term “health data”**.

The term **“Health Information Exchange” (HIE)** is defined as the electronic mobilization of health information across organizations and disparate systems within a region or community. The goal of a health information exchange is to support interoperability and facilitate access to and retrieval of clinical data, privately and securely, to provide safer, timelier, efficient, effective, equitable patient-centered care.⁵ In all project materials, the term **“health information exchange” is used synonymously with the terms: “Regional Health Information Organization” (RHIO) and “Health Information Network”**.

A health information exchange may be a very simple arrangement between two health care organizations or a more complex arrangement with many participating organizations. The following pictures identify and describe two possible types of health information exchanges.

Figure 1 shows a simple health information exchange between two organizations: Independent Hospital and Health System A. The organizations may want to exchange a limited amount of data to address a specific community need. For example, they may want to enable Independent Hospital to access Health System A’s data for patients who present in the emergency department after normal clinic hours. The key characteristics of this exchange include:

Figure 1 – A Simple Model of Health Information Exchange



The organizations may want to exchange a limited amount of data to address a specific community need. For example, they may want to enable Independent Hospital to access Health System A’s data for patients who present in the emergency department after normal clinic hours. The key characteristics of this exchange include:

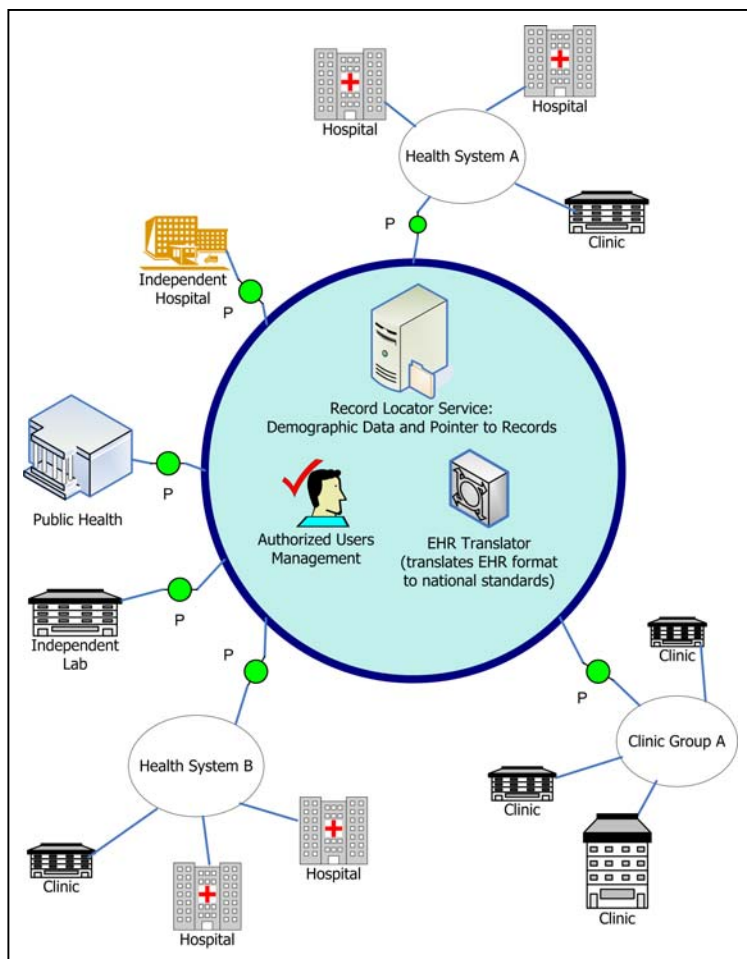
- Decentralized data – Each organization maintains its own data on its own systems;
- User authorization and access is coordinated directly between the organizations, and in the example may be limited to emergency department physicians and nurses;
- Patient identification is coordinated between the organizations and there is no centralized record locator service; and
- Access to the other organization’s electronic health record may be:
 - Full read/write access;
 - View only access; or

⁵ This definition is an adaptation the e-Health Initiative’s definition. See <http://www.ehealthinitiative.org/>

- o The exchange of clinical messages that contain specific clinical data (e.g., continuity of care record, medication history, etc.).

In contrast, Figure 2 shows a significantly more complex health information exchange that involves multiple participants. This type of health information exchange is consistent with a community-wide exchange intended to ensure that all health care providers treating a patient are capable of accessing the information necessary to provide appropriate treatment. The characteristics for this type of health information exchange are:

Figure 2 – A Complex Model of Health Information Exchange



- Decentralized Data – Each organization maintains its own data on its own systems;
- User authorization and access is coordinated centrally;
- Patient identification is coordinated centrally through a record locator service that contains patients’ demographic data and a pointer to the locations of patients’ clinical data;
- Access to the electronic health record is limited to health information published to a front-end portal. The portals may be limited to such information as:
 - o Medical history
 - o Medication history
 - o Continuity of care documents

As seen from the two examples, the number of participants, the amount and types of information exchanged, and the

need for centralized coordinated administrative services can vary significantly between health information exchanges. This report is not recommending a particular model for a health information exchange, but rather presents the range of possibilities to aid in ensuring that the analysis of privacy and security issues is broad enough to encompass them.

The term “**patient**” and “**consumer**” are used interchangeably within this document.

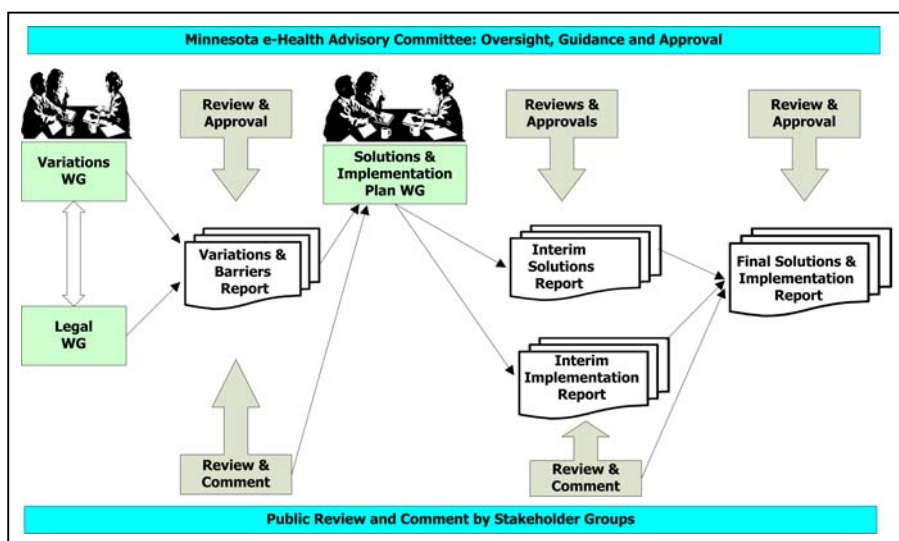
PROJECT METHODOLOGY

PROJECT STRUCTURE

Stakeholder and consumer involvement are critical to ensuring that the MPSP's results are applicable to the community as a whole and to ensuring broad acceptance. Accordingly, the MPSP is structured to provide all interested stakeholders the ability to participate in the project and follow the project activities through the MPSP website⁶. The overall project structure is shown in Figure 3.

The project is under the general guidance of the Minnesota e-Health Advisory Committee, which serves as the steering committee for the project's work. The detailed analytical activities of the project are being carried out through three Work Groups appointed by the MN e-Health Advisory Committee:

Figure 3 – MPSP Structure



The detailed analytical activities of the project are being carried out through three Work Groups appointed by the MN e-Health Advisory Committee:

- **Variations Work Group**
- **Legal Work Group**
- **Solutions and Implementation Plans Work Group**

Variations Work Group

The Variations Work Group consisted of privacy and security experts that represent health systems, health plans, hospitals, public health agencies, local units of government, and other organizations involved in the exchange of health information. A listing of individuals and organizations participating in the Variations Work Group can be found in Appendix A. The privacy and security experts provided representation in three broad areas:

- Privacy Officers responsible for developing and implementing privacy policies and procedures that address patient privacy protections and patient rights in the use and disclosure of health information.
- Chief Information Officers/Security Officers responsible for developing and implementing security policies and procedures that address the confidentiality, integrity and availability of health information.

⁶ (<http://health.state.mn.us/e-health/mpsp/>)

- Other subject experts (e.g., health information managers) with routine responsibility for data exchanges and who understand the daily operational challenges of data exchange between disparate information systems within and between organizations.

This work group was responsible for identifying and assessing privacy and security issues that create practical barriers to the appropriate exchange of health information. This group was also responsible for evaluating variations in organization-level business policies and practices in order to assess their impact on the development and implementation of a health information exchange.

Legal Work Group

The Legal Work Group consisted of legal experts representing consumers, health systems, health plans, hospitals, public health agencies, and other organizations involved in the exchange of health information. A listing of individuals and organizations participating in the Legal Work Group can be found in Appendix A. The legal experts provided representation in three broad areas:

- Privacy Officers/Compliance Officers responsible for developing and implementing privacy policies and procedures that comply with legal requirements that protect privacy and patient rights.
- Legal Counsel responsible for interpreting and implementing state and federal requirements for protecting health privacy and patient rights.
- Other subject experts with routine responsibility for advocating for consumer privacy rights and patient protections.

This work group was responsible for identifying the legal and regulatory rationale underlying the business practices that were identified as privacy and security barriers to the development and implementation of health information exchanges. The group also spent significant time discussing and analyzing Minnesota's patient consent requirements in Minnesota Statutes § 144.335.

Solutions and Implementation Plan Work Group

The Solutions and Implementation Plan Work Group is being formed while this report is written. The work group will consist of approximately 40 individuals representing consumers, health systems, health plans, hospitals, public health agencies, tribal clinics and other organizations involved in the exchange of health information. The work group members will provide representation in three broad areas:

- The development and implementation of privacy policies and procedures that protect patients' privacy and rights in the use and disclosure of health information;
- Information systems development and the implementation of security policies and procedures addressing the confidentiality, integrity and availability of health information; and
- Consumer and patient advocacy.

This work group will have two responsibilities. First, the work group will develop solutions to eliminate or reduce the most significant privacy and security barriers impeding the exchange of health information, while preserving and strengthening patient privacy protections. Second, the work group will create an action plans to implement the solutions identified and developed in response to the privacy and security barriers identified in this report.

PROJECT ACTIVITIES

Analyzing Situational-Based Scenarios

One of the MPSP's major activities was the Variations Work Group's analysis and evaluation of 18 scenarios developed nationally for the HISPC contract. The scenarios represent a wide range of purposes for exchanging health information across a broad array of health care organizations and were intended to provide a standardized context for discussing organization-level business practices across all states and territories. The scenarios are situational-based and generally describe an exchange of health information within a particular context where privacy and security barriers were considered likely. The national project also identified nine privacy and security domains for classifying business practices and privacy/security issues.

Because the scenarios were developed for use by all 34 states and territories with a HISPC contract, they needed to be adapted to be consistent with Minnesota's health care delivery systems. Additionally, staff identified "key issues" and "questions for consideration" for each scenario to structure the Variation Work Group' discussion and analysis of the scenarios. The key issues identified were the aspects of the scenarios that were anticipated to be most significant, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members' organizations. The 18 scenarios, key issues, and questions for consideration are presented in Appendix C and the nine privacy and security domains are presented in Appendix B.

The Variations Work Group analyzed and discussed the scenarios over the course of seven meetings. The 2.5 hour meetings were held between June 14, 2006 and September 13, 2006. The analysis and discussion of each scenario was documented (see Appendix D) to:

- Present the scenario, key issues, likely privacy and security domains, and questions for consideration;
- Describe the general business processes used by Variations Work Group members' organizations in addressing the exchange of health information within the scenario; and
- Identify other issues related to the privacy and security domains not otherwise covered in the general business processes section.

It was anticipated that the business practices identified by the Variations Work Group would need to be reviewed by the Legal Work Group in order to identify legal and regulatory rationale underlying the business practices. However, Variations Work Group members were generally able to provide the legal and regulatory rationale directly as part of the overall discussion.

Although the Variations Work Group reviewed all 18 of the scenarios, some of the scenarios were first reviewed and analyzed by ad-hoc groups of stakeholders more directly associated with the scenario. For example, Scenario #15 dealt with the Minnesota Department of Health's disclosure of information related to an active case of tuberculosis. Therefore, Scenario #15 was first analyzed by the Tuberculosis Unit within the Minnesota Department of Health's Infectious Disease Epidemiology, Prevention and Control Division and then provided to the Variations Work Group. Scenarios #13, 16, and 18 were also first reviewed by an ad-hoc group, before presentation to the Variations Work Group.

Examining Current and Emerging Models of Health Information Exchanges

Both the Variations Work Group and the Legal Work Group were asked to analyze current and emerging models of health information exchanges to identify potential privacy, security, and/or legal barriers to exchanging information. The work groups were asked to identify privacy, security, and legal concerns based on:

- Their organizations' experiences in implementing electronic health records within their own organizations; and
- The privacy, security and legal concerns and issues encountered as their organizations have attempted to electronically exchange health information with other health care organizations.

The work groups' discussions of various models of health information exchange differed from the discussion of the scenarios. The scenarios focused on how health information was currently being exchanged regardless of media (i.e., paper or electronic). The discussion of models of health information exchange focused on the privacy and security concerns facing health care organizations in their current endeavors to implement electronic exchanges of information. These discussions were valuable in that they revealed that the most significant barriers to the electronic exchange of health information are often the health care organizations' inability to find any fully adequate solutions for addressing their concerns.

In-Depth Analysis of Patient Consent Requirements

Minnesota's requirements for patient consent to release health information were identified early in the project as a potential barrier to the development and implementation of health information exchanges. Minnesota's patient consent requirements are significant in their impact on health care organizations' ability to electronically exchange health information because the requirements generally apply to all health information, to all health care providers, and to all exchanges of information, including treatment. In general, when Minnesota health care providers consider any disclosure/exchange of patients' health data, their analysis usually begins with the question, "Has our organization complied with all relevant patient consent requirements for releasing the information?"

The issue of patient consent requirements is so significant that it essentially serves as a precondition for the electronic exchange of health information. Consequently, it is imperative that health care organizations are able to operationally implement patient consent requirements as part of the electronic exchange of information; otherwise, many of the other privacy and security issues will become irrelevant as organizations will be unwilling to modify paper processes that have already integrated the consent requirements.

To ensure that the project had a complete and accurate understanding of patient consent issue, the legal work group spent the majority of its time (i.e., 5 meetings, each 2.5 hours in length) discussing Minnesota's patient consent requirements and liability concerns. The discussions attempted to:

- Document ambiguities in the requirements and their impact on the exchange of information;
- Identify and describe variations in organizations' interpretations of the requirements and how the variations impact the implementation of patient consent;
- Assess how the requirements would apply to various aspects of a health information exchange's activities; and
- Determine how organizations' concerns about liability for inappropriate disclosures of patient data impact the implementation of patient consent and the ability to achieve real-time, electronic exchange of health information.

PRIVACY AND SECURITY BARRIERS TO THE ELECTRONIC EXCHANGE OF HEALTH INFORMATION

INTRODUCTION

The Variations Work Group and the Legal Work Group spent a significant amount of time discussing and reviewing issues associated with the exchange of health information – both electronically and on paper. The Work Groups' activities included:

- Analyzing situational-based scenarios, which investigated organizations' policies, practices, and mechanisms for exchanging health information;
- Discussing privacy and security issues identified by organizations as part of their internal implementation of electronic health records;
- Describing privacy and security issues encountered when organizations have attempted to electronically exchange health information with other organizations;
- Examining current and emerging models of health information exchanges and identifying privacy and security concerns related to the exchange of information in these models; and
- Investigating thoroughly organizations' interpretation and implementation of Minnesota's patient consent requirements.

The original premise of the project was that significant variations across organizations' business practices for handling and disclosing health information are a significant barrier to exchanging data. However, the premise was not supported by the work groups' analyses. In general, and with the notable exception of patient consent, the project did not find significant variations in business practices across organizations. Indeed, most organizational variation identified was not deemed a significant impediment to the appropriate exchange of health information.

The MPSP revealed that the real privacy and security issues impeding the electronic exchange of health information are universal, overarching issues that impact all types of health care organizations and apply to all types of health information. Throughout all of the project's activities, the same issues were repeatedly identified as the major privacy and security concerns that represent serious impediments to advancing the electronic exchange of health information. Many of these privacy and security issues do not arise because organizations have different business practices. Rather, they are an impediment because organizations have not found any fully adequate mechanisms to address the issues.

The overarching privacy and security issues that must be solved to advance the appropriate electronic exchange of health information can be grouped into three general categories:

1. **The implementation of Minnesota's patient consent requirements within a health information exchange.** This issue has two parts. First, there are significant and irreconcilable differences in organizations' interpretations of Minnesota's patient consent requirements. These differences make it impossible for health care providers to agree on "when" and "how" patient consent is required. Second, the patient consent requirements were designed for the paper-based exchange of information or for early electronic data base systems and are not conducive to a real-time, automated electronic exchange of information. The Minnesota's patient consent

requirements are particularly significant because they apply to all health information, to all health care providers, and to all exchanges of information, including treatment.

2. **Operational difficulties in first providing, and then limiting and monitoring external organizations' electronic access to patient data.** This issue is identified as one general issue, because it is a set of interconnected security problems that must be addressed concurrently to successfully implement a health information exchange. To give external health care providers appropriate access to electronic health records and patient data, organizations need to address four security topics:
 - a. Mechanisms to establish and maintain a list of individuals authorized to access patient data;
 - b. Methods to authenticate authorized individuals when accessing patient data;
 - c. Information system access controls and coordinated access control policies to limit authorized individuals' access to patient data appropriate to the individual's functions and needs; and
 - d. Mechanisms for coordinated auditing across organizations to identify authorized individuals who may have inappropriately accessed health information.
3. **Liability concerns with the inappropriate disclosure of patients' health information.** Health care organizations face liability from various sources for the inappropriate disclosure of patient data. Consequently, health care organizations are cautious in their approach to exchanging data. Health care organizations explicitly consider organizational risk as a factor in their decision to participate in a health information exchange. That is, they want to be confident that the health information exchange has appropriately addressed privacy/security issues to minimize their organization's liability from inappropriate disclosures of patients' data.

A final recurring theme in both Work Groups was patient/consumer issues. Participants stated emphatically that any health information exchange must be designed to address patients' needs, interests, and concerns. They said that successfully addressing patient/consumer issues is critical to ensuring the successful implementation of health information exchanges. In fact, the Work Groups were less concerned about patient/consumer issues serving as a barrier and more concerned about ensuring that we can accurately identify and understand patients' issues, needs, and concerns.

CONSUMER TRUST AND ACCEPTANCE OF HEALTH INFORMATION EXCHANGES

The Variations and Legal Work Groups believe consumer acceptance and trust must serve as the foundation for a health information exchange's successful development and implementation. The privacy and security protections afforded to patients' health information are important factors in earning that trust. One key privacy protection is Minnesota's patient consent law. Consent gives patients control over which health information can be shared with whom. Therefore, patients and consumers have a strong interest in how patient consent requirements are defined and implemented within health information exchanges. Thus, it will be important to ensure that consumers' perspectives are included in addressing the patient consent issues identified later in this report.

The Variations and Legal Work Groups also identified education as a critical component in developing consumer acceptance of health information exchanges. Patients will need to understand how they will benefit from making their health information available to their providers through a health information exchange. If patients do not perceive health information exchanges as facilitating and improving their health care experience, they may be reluctant to make their data more electronically available. Likewise, if patients are

concerned about the security and privacy of their health information, they are unlikely to accept health information exchanges.

Patient consent and consumer education come together in a number of ways. Many Work Group members believe that, despite the difficulty of incorporating Minnesota's patient consent requirements into the operations of a health information exchange, the consent process and documents used to obtain patients' consent can serve as primary education tools to aid patients in understanding the benefits of a health information exchange. Educational materials and forms used in the patient consent process help to establish reasonable expectations concerning the privacy, security and accessibility of electronic health records and permit patients to ask questions about the protections afforded their health data. Providing information and materials in formats and media that are easy for patients to understand will be a major undertaking. Distilling technical information so that the benefits and processes of a health information exchange are accurately reflected is an additional hurdle. Even with these challenges, Variations and Legal Work Group members expect consumer education to be a necessary and integral part of successful health information exchange implementation.

One of the goals of both the consumer education and patient consent processes should be to make the health information exchange's privacy protections understandable and transparent. That is, patients should be able to easily understand:

- How to provide and revoke consent for exchanging their health information among providers;
- How information will be exchanged and made available to their health care providers when they sign various consents;
- The impacts of consent on the handling of their data and their providers' abilities to deliver care; and
- What other privacy and security protections are in place to maintain the confidentiality of their data.

During the Work Group discussions, two specific consumer interests were identified. First, consumers want the ability to know who has accessed their health data. Consumers and others believe that as health information is increasingly stored, accessed, and exchanged electronically, it should become easier for health care providers to maintain a log of who has accessed their data. Consumers expressed a strong interest in being able to request the log of people and organizations that have electronically accessed their health information. While all Work Group members' organizations maintain audit logs that record when patients' data are accessed, most Work Group members did not think that it was currently practical or feasible to provide the information to consumers. The information may be undecipherable without knowing an organization's business practices and workflow, it may be unintelligible without access to other data sources, and it is unlikely to aid a patient in knowing if their data has been inappropriately accessed. Health care organizations on the Work Groups agree that it is important to have mechanisms to determine if patients' data have been inappropriately accessed. Yet, their experience in using audit logs suggests that the logs will not easily address the consumers' concerns. However, all Work Group members agree that with improved technology and enhanced capacity to intelligently track access, there will be greater ability to assist consumers in knowing who has accessed their data and why it was accessed.

The second specific consumer interest identified was the desire to be notified when there is a breach in the security of their health information. Recently, Minnesota law was amended to remove an exception for HIPAA-covered entities from the requirement that consumers be notified of security breaches. As consumers regularly learn of computer security breaches through newspapers and other media, they are increasingly worried about the overall security and privacy of their personal information. While notification of a breach in security does little to proactively protect the data, it will provide an additional incentive for organizations to

implement appropriate security measures to avoid the breach. The notification will also help consumers know when and how their data has been disclosed and what steps they can take to mitigate the possibility of identity theft or other harm. Hence, consumer notification for security breaches will be important for creating consumer acceptance of electronic storage and exchange of health information.

MINNESOTA'S PATIENT CONSENT REQUIREMENTS - GENERAL

Background: Patient Consent Requirements in Minnesota Statutes

Minnesota has a single statute that governs health care providers' release/disclosure of most health information. Minnesota Statutes § 144.335 (the Medical Records Act) gives patients control over their health care providers' release of patient-identified health information. The Minnesota provisions are generally more stringent than the protections in the Health Insurance Portability and Accountability Act (HIPAA) Privacy regulations (45 CFR Part 164). Government health care providers must also comply with additional requirements detailed in Minnesota Statutes, Chapter 13 (the Minnesota Government Data Practices Act). However, the Legal Work Group and this report has focused its attention on Minnesota Statutes § 144.335 because it applies to the release of health records by all health care providers and, in the absence other more specific laws, applies to all health information.

The majority of issues discussed and referenced in the report's next sections are related to this significant portion of Minnesota Statutes § 144.335, subdivision 3a:

Subd. 3a. Patient consent to release of records; liability. (a) *A provider, or a person who receives health records from a provider, may not release a patient's health records to a person without a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release, unless the release is specifically authorized by law. Except as provided in paragraph (c) or (d), a consent is valid for one year or for a lesser period specified in the consent or for a different period provided by law.*

(b) *This subdivision does not prohibit the release of health records:*

- (1) *for a medical emergency when the provider is unable to obtain the patient's consent due to the patient's condition or the nature of the medical emergency; or*
- (2) *to other providers within related health care entities when necessary for the current treatment of the patient.*

(c) *Notwithstanding paragraph (a), if a patient explicitly gives informed consent to the release of health records for the purposes and pursuant to the restrictions in clauses (1) and (2), the consent does not expire after one year for:*

- (1) *the release of health records to a provider who is being advised or consulted with in connection with the current treatment of the patient;*
- (2) *the release of health records to an accident and health insurer, health service plan corporation, health maintenance organization, or third-party administrator for purposes of payment of claims, fraud investigation, or quality of care review and studies, provided that:*
 - (i) *the use or release of the records complies with sections 72A.49 to 72A.505;*

(ii) further use or release of the records in individually identifiable form to a person other than the patient without the patient's consent is prohibited; and

(iii) the recipient establishes adequate safeguards to protect the records from unauthorized disclosure, including a procedure for removal or destruction of information that identifies the patient.

Release versus Exchange of Health Records

As the statutory language shows, section 144.335, subdivision 3a focuses and defines patient consent requirements in terms of the "release of health records", rather than the "exchange of health records." The importance of this focus is subtle, but significant. By defining the consent requirements in relation to a "release of health records", the statute uses a framework that primarily contemplates only two actors in the activity - the patient and the discloser of the health records. Thus, the statute places all responsibilities, requirements, and liability for the appropriateness of data exchange on the discloser of health records.

The concept of a health information exchange is built on a framework that contemplates at least three actors in the activity - the patient, the discloser of the health records, and the requestor of the health records. A health information exchange anticipates that all of the actors involved in an exchange have responsibilities, requirements, and liability for ensuring the appropriateness of the exchange of information.

Later sections of the report discuss issues arising from this statute's focus on "release" versus a health information exchange's focus on "exchange." At this point, it is sufficient to note that the concept of exchanging health records is a more expansive framework for thinking about the appropriate sharing of patients' health data.

The Impact of Patient Consent on a Health Information Exchange

Minnesota's patient consent requirements impact health care providers' ability to exchange health information and form barriers to the development of a health information exchange in three distinct areas:

1. The methodologies used to locate patients' health records;
2. The ability to determine when patient consent is necessary for health care providers to exchange patients' health information; and
3. The processes for how patient consent is integrated into health information exchanges' activities.

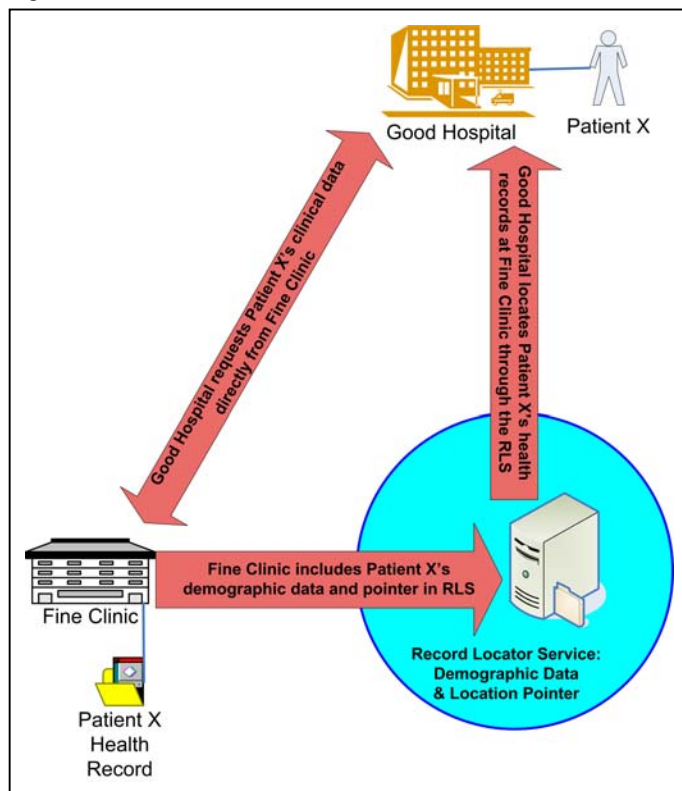
IMPACT OF MINNESOTA'S PATIENT CONSENT REQUIREMENTS ON LOCATING PATIENTS' HEALTH INFORMATION

When a health care provider needs to obtain a patient's health information from other providers, their first task is to locate those providers who have the pertinent information. A health information exchange requires some method of locating patients' health information. One seemingly simple method of locating health records is to ask patients to identify the location of their health information. However, there are situations when the patient cannot be of assistance. The patient may be unconscious, not physically present, or unable to accurately remember where health care has been received in the past.

Given that patients may be unable to correctly and effectively identify the location of their records, many health information exchanges contemplate the use of some type of record locator service (RLS). A record locator service functions as an index or card catalog for patient records; the RLS stores sufficient demographic data to uniquely identify each patient and provides pointers to the locations of patients' health information. The RLS only contains the demographic data necessary to assist providers in finding the location

of all pertinent health information; it does not contain the patients' clinical data. Once a provider locates a patient's records through the RLS, the exchange of appropriate clinical data would need to occur between the specific health care providers. Figure 4 illustrates the use of an RLS and the different flow of RLS data and clinical data.

Figure 4 – A Record Locator Service



Initially, the Work Group assumed that the demographic data for a record locator service could be limited to those elements identified in the Markle Foundation's *The Connecting for Health Common Framework*. That framework limits the elements to:

- First and Last Name
- Date of Birth
- Gender
- Zip Code
- Pointer to the Records

However, during the analysis of a number of the scenarios and based on participants' experiences in matching records, the Variations Work Group concluded that the RLS would need to have more demographic data to uniquely identify patients. Even with additional demographic data, there may be problems in uniquely identifying certain populations with common or frequently used names such as Maria Martinez or Robert Johnson. In particular,

many immigrants share common names and use January 1 as a proxy for an unknown birth date.

Minnesota's Patient Consent Requirements for a Record Locator Service

The first issue to be addressed by a health information exchange in establishing a record locator service is determining whether:

1. Patient consent is required for a health care provider to submit patients' demographic data and a pointer to the location of the health records to an RLS; and
2. Current patient consent restrictions, such as the one-year time limit on consents, apply to a record locator service.

To determine whether patient consent is needed to include patients' demographic data and a pointer in an RLS, a provider needs to know whether:

- A patients' demographic data and a pointer to the location of information is a "health record" under section 144.335, subdivision 3a; and
- Providing demographic data to an RLS is "a release" under subdivision 3a.

RLS Data, Health Records and Patient Consent

Are patients' demographic data and a pointer to the location of patients' health information a "health record" under Minnesota law? The Legal Work Group members were split on this question, as Minnesota law does not define the term "health record."

Generally, in the absence of a definition, Minnesota rules of statutory construction direct the reader to the plain or common meaning of a term and thus to the dictionary. In this instance, the common or dictionary meaning of the phrase "health record" is not helpful because there is substantial latitude in the definition of those terms. In addition, some healthcare providers use "health records" as a term of art, which is a word or phrase used by professionals that has a precise meaning in a particular subject area. Interestingly, it appears that, while there is no agreement on the precise definition of "health record," some providers believe that the term covers less data than might be covered by a "plain meaning" analysis.

Some Work Group members looked to HIPAA's definitions of "individually identifiable health information" and "protected health information" for guidance in defining "health records." For a health care provider required to comply with HIPAA, patient demographic data combined with a pointer to records are clearly protected health information. Some Work Group members argued that the terms "health records" and "protected health information" should be considered synonyms and consequently, the RLS information should be considered a health record.

Other Legal Work Group members argued that the terms "health records" and "protected health information" should not be considered synonyms because the data for an RLS do not generally reveal information about the patient's health. If this is so, then they asserted that providers would not need patients' consent to include the data in an RLS.

However, all members agreed that, in certain circumstances, the RLS data could reveal information about the patient's health. For example, if the patient had a health record at a location that only provided substance abuse treatment or only provided mental health treatment, then the RLS data would reveal information about the patient's health.

In the end, the Legal Work Group was unable to definitively answer the question, "Are patients' demographic data and a pointer to the location of patients' health information a health record under Minnesota law?"

Is providing an RLS patients' demographic data and a pointer to the location information a "release" under Minnesota law? Legal Work Group members generally agreed on the answer to this question. If there is a contractual relationship between the provider and RLS (i.e., the RLS is an agent of the provider) simply providing data to the RLS is not a release. However, once another provider accesses the RLS data, then there has been a release to that other provider. Hence, simply loading patients' data into an RLS is not a release when there is a contractual relationship, but allowing other providers to utilize the data to find patients' records is a release of information.

The creation and use of a record locator service requires health care providers to agree on "when" and "how" patient consent must be used to provide and access RLS data. The fact that Minnesota Statutes do not define the term "health records" leads health care providers to disagree about whether or not RLS data are health records. This leads to further disagreement about when patient consent is needed to provide and access RLS data.

Thus, the first barrier created by Minnesota's consent requirements is the inability to determine if consent is needed to develop an RLS. This barrier could be eliminated by amending section 144.335, subdivision 3a and its related definitions to clearly indicate if:

- Patients' demographic data and a pointer to the location of patients' health information constitutes a health record; and/or

- Patient consent is required to include patients' demographic data and a pointer to the location of patients' health information in a record locator service.

RLS Data and Time Limits on Patient Consent

Under section 144.335, subdivision 3a, a patient's consent for the release of health information lasts for one year except in special circumstances. Whenever the patient's consent is required to include data in an RLS, the patient's consent will expire in one year, unless the patient's consent fits into one of the exceptions.

This issue highlights another ambiguity in Minnesota's patient consent requirements and the second potential barrier to the use of an RLS. Legal Work Group members disagreed on whether or not a patient's consent to include data in an RLS fits into one of the exceptions to the one-year time limit. The cause of the ambiguity and disagreement is the fact that Minnesota Statutes do not define the term "current treatment".

Section 144.335, subdivision 3a, (c)(1) states that consent does not expire for "the release of health records to a provider who is being advised or consulted with in connection with the current treatment of the patient." Some Legal Work Group members argue that as long as the health information exchange is only for patient treatment, then the patient's consent can be fit into this exception. However, other Legal Work Group members argue that, under their interpretation, of "current treatment" the consent for the RLS would expire in one year. The impact of these different interpretations for the term "current treatment" is addressed later in the report, where its impact is more significant.

An annual renewal of the patient's consent to include data in an RLS would be operationally difficult and costly, particularly for patients that a provider may not have seen in the previous year. Additionally, providers would need to create mechanisms and processes to continually add and remove data from the RLS as patients' consents expire, are revoked, and/or are renewed. This constant turnover in the RLS may not be reflective of patients' desires, but rather:

- The short time frame for consent efficacy; and
- The difficulty of continually renewing consents—because patients see providers on an as-needed basis that may not conveniently coincide with the renewal anniversary.

The purpose of an RLS is to give health care providers an efficient and effective method of correctly identifying the location of patients' health records. If a patient is unable to consent to including their demographic data for more than one year and there are not effective processes to manage patients' consents for including data in an RLS, then the RLS will not be:

- A complete and accurate method of locating patients' records;
- Convenient for the patient who needs to continually renew an ever-increasing number of consents; or
- Cost effective for providers needing to continually renew patients' consents.

This second potential barrier created by Minnesota's consent requirements – the inability to cost-effectively maintain a complete and accurate RLS – could be eliminated by amending section 144.335, subdivision 3a, and its related definitions to clearly indicate:

- Once again, if patient consent is required to include patients' demographic data and a pointer to the location of patients' health information in a record locator service; and
- If so, then whether this RLS consent expires within one year.

Conclusion: Barriers to an RLS Resulting from Minnesota's Patient Consent Requirements

Implementing a health information exchange and record locator service requires health care providers to agree on "when" and "how" patient consent will be used to exchange and share patient data. This agreement is necessary to ensure that all providers participating in the health information exchange employ common policies and procedures to protect the privacy of their patients' information.

Ambiguity in Minnesota's patient consent requirements form a number of barriers to the creation and use of a record locator service:

1. Minnesota Statutes do not define the term "health record." Consequently, there is disagreement about whether or not RLS data are health records and require patient consent for their inclusion in a record locator service.
2. Minnesota Statutes do not define the term "current treatment." Consequently, there is disagreement about whether or not any patient consent required to include data in an RLS expires after one year and needs to be renewed annually.
3. If patients are unable to consent to their data being in an RLS for more than one year, the RLS will not be a complete and accurate method for locating patients' records.
4. Managing a process to annually renew patient consents to include data in an RLS will be costly and operationally difficult for health care providers, particularly for those patients that have not been seen in the previous year.
5. Patients may find it burdensome to continually need to renew an ever-increasing number of consents to ensure that providers can accurately locate their health records.

**IMPACT OF MINNESOTA'S PATIENT CONSENT REQUIREMENTS
ON THE EXCHANGE PATIENTS' HEALTH INFORMATION**

Minnesota law requires patient consent for the release of health information even if the release is to another health care provider for patient treatment and certain statutory exceptions are not met. Therefore, any health information exchange developed to electronically exchange health records between health care providers must address two fundamental issues:

1. When is patient consent required to disclose data to another health care provider for patient treatment?
2. How should patient consent be obtained?

These questions not only need to be addressed, but providers must agree on the answers for a health information exchange to succeed. If providers cannot agree when consent is needed, then they will not have a common foundation for agreeing on other essential issues such as:

- Determining the policies and procedures that health information exchange participants need to collectively implement to appropriately protect the privacy of patients' health information;
- Determining how Minnesota's patient consent requirements will be operationally implemented in the health information exchange to ensure that patients' desires are honored;

- Determining if any particular exchange of health information is appropriate and permitted under Minnesota law;
- Communicating with patients about the mechanisms that permit them to control the disclosure of their health information; and
- Explaining to patients when and how their health information can be disclosed.

During Legal Work Group discussions of the two fundamental issues, it was clear that providers do not all have the same interpretation of the statutory language. In particular, they do not agree on when consent is needed or how the consent should be obtained. Specifically, different interpretations of the following undefined terms lead to fundamentally different interpretations of Minnesota’s statutory requirements:

- Current Treatment
- Medical Emergency
- Related Health Care Entity

Two Views of “Current Treatment” and the Impact on Patient Consent Requirements

Minnesota Statutes, section 144.335, subdivision 3a, states that a patient’s consent is valid for no longer than one year. However, the statute provides an exception to the one-year time limit in paragraph (c), where it states:

(c) Notwithstanding paragraph (a), if a patient explicitly gives informed consent to the release of health records for the purposes and pursuant to the restrictions in clauses (1) and (2), the consent does not expire after one year for:

(1) the release of health records to a provider who is being advised or consulted with in connection with the current treatment of the patient;

Almost all health care providers respond to this portion of the statute in the same way. During a patient’s initial visit, providers ask the patient to complete a general consent for the release of health records to providers who are being advised or consulted with in connection with the patient’s current treatment. This general consent does not expire, but may be revoked at any time.

To understand when the general consent permits a health care provider to release health records to another provider, it is necessary to understand what is included in the term “current treatment.” Unfortunately, the statutes do not define the term “current treatment.” Consequently, health care providers have adopted at least two different interpretations for the term with very different implications:

- **Interpretation 1:** This interpretation holds that the general consent permits the provider to disclose any health information at any time to any provider who is currently treating the patient. Note: Any health information means information not covered by another law (e.g., substance abuse treatment data and genetic data).

This first interpretation reads subdivision 3a, (c)(1) as though the statute were written as:

(1) the release of health records to a provider who is ~~being advised or consulted with~~ in connection with the current treatment of currently treating the patient;

- **Interpretation 2:** This interpretation holds that the general consent only permits the provider to disclose health records to other providers being advised or consulted in relation to the releasing provider’s current treatment of the patient (e.g., for continuity of care or referrals).

This second interpretation reads subdivision 3a, (c)(1) as though the statute were written as:

(1) the release of health records to a provider who is being advised or consulted with in connection with the releasing provider's current treatment of the patient;

These two different interpretations yield substantially different answers to our questions of when patient consent is needed and how it should be obtained. These differences are illustrated in the following example:

Patient X has hip replacement surgery at Good Hospital. As part of the admission paperwork, Patient X signs a general consent that permits Good Hospital to release Patient X's health records to providers being advised or consulted with in connection with Patient X's current treatment. After the surgery, Patient X is referred to Fine Rehabilitation Center for physical therapy associated with the hip replacement. Good Hospital and Fine Rehabilitation Center are unrelated and are not under common ownership.

Two years after hip surgery, Patient X injures his knee and visits Superior Clinic. The doctors at Superior Clinic would like to get Patient X's health records from Good Hospital to have a more complete understanding of the overall situation with Patient X's knee and leg. Superior Clinic is unrelated and not under common ownership with Good Hospital or Fine Rehabilitation Center.

When and How Patient X's Consent is Obtain to Exchange Health Records		
Providers Exchanging Patient X's Health Records	Interpretation 1	Interpretation 2
From Good Hospital to Fine Rehabilitation Center	<p>The general consent obtained at admission to Good Hospital is sufficient, because Fine Rehabilitation Center is now <u>currently treating</u> Patient X.</p> <p>No additional or more specific consent is needed.</p>	<p>The general consent obtained at Good Hospital is sufficient because Patient X <u>is being referred</u> to Fine Rehabilitation <u>by Good Hospital</u> in connection with the hip surgery.</p> <p>No additional or more specific consent is needed.</p>
From Good Hospital to Superior Clinic	<p>The general consent obtained two years earlier at Good Hospital is sufficient consent, because Superior Clinic is now <u>currently treating</u> Patient X.</p> <p>No additional or more specific consent is needed.</p>	<p>Good Hospital would require Patient X to provide a written consent that specifically authorizes Good Hospital to release Patient X's health records to Superior Clinic. Patient X's care at Superior Clinic is <u>not part of the care that was being provided by Good Hospital</u> and is therefore <u>not covered by the general consent</u> obtained at Good Hospital.</p> <p>This new, specific consent is valid for no more than one year.</p>

In the example, when patient consent is required (or at least when specific patient consent versus general patient consent is required) depends on whether a provider adheres to Interpretation 1 or Interpretation 2.



To appreciate the practical difficulties that can arise in exchanging Patient X's health records, imagine that Good Hospital adheres to Interpretation 2 and Superior Clinic adheres to Interpretation 1. That situation raises the following difficult questions concerning the exchange of Patient X's health records:

- How will Superior Clinic know if a specific consent from Patient X is needed for Good Hospital to release the records the clinic has requested?
- How will Superior Clinic know what advice to provide Patient X about actions to take to ensure that the clinic has the appropriate records for Patient X?
- How will Superior Clinic know if it should assist Patient X in completing a patient consent for the requested records?
- How will the electronic exchange of information be automated if the parties to the exchange cannot agree on the requirements for the exchange to occur?

Without a definition of "current treatment" and without agreement on the appropriate interpretation of section 144.335, subdivision 3a, (c)(1), it will be difficult to get widespread agreement on when and how patient consent is required within a health information exchange. The wide spectrum covered by the providers' interpretations of "current treatment" means that Minnesota does not have a uniform foundation on which to build its electronic health information exchange efforts. This lack of a common foundation will complicate and delay the development of electronic exchange and create variability in patients' privacy protections.

Definition of "Medical Emergency" and the Need for Patient Consent

Section 144.335, subdivision 3a provides two additional exceptions to the patient consent requirements. The first exception is during a "medical emergency", although there is no statutorily-based definition for the term.

As noted earlier, in the absence of a specific definition, Minnesota's rules of statutory construction direct the reader to the plain meaning of the term and thus to the dictionary. However even with these directions, health care providers do not universally agree on whether or not specific situations are considered medical emergencies. Providers generally agree on the emergency nature of situations when immediate medical care is necessary to:

- Preserve life;
- Prevent serious impairment to bodily functions; or
- Prevent placing the patient's physical or mental health in serious jeopardy.

However, providers do not always agree on the emergency nature of situations that test the boundaries of the definition, for example:

- A dazed and confused patient shows up in the emergency department, although the patient's life and body function are not in immediate danger; or
- A patient is brought to the emergency department unconscious, but in stable condition.

The health care provider releasing a patient's health records bears all responsibility for ensuring that the release of records is appropriate and permitted under law. Consequently, prior to releasing a patient's health records, the releasing provider generally needs to make some assessment that the patient is in a medical emergency and unable to provide consent. When the releasing provider and the treating provider disagree about the emergency nature of the patient's situation, they will also disagree about the need for patient

consent to release records. Agreement on a definition for “medical emergency” would provide clarity for this exception to the consent requirement and would benefit:

- Patients, by helping to ensure that their health information is available during medical emergencies;
- Providers, by furnishing a single definition of medical emergency to aid in uniformly determining the appropriateness of releasing health records without consent; and
- Health information exchanges, by facilitating agreement about when patient consent is needed to exchange information.

Definition of “Related Health Care Entities” and the Need for Patient Consent

The second exception to the consent requirement is when the release is within a “related health care entity.” Minnesota Statutes do not define the term “related health care entity,” although most health care providers interpret the term to mean organizations owned and operated by the same legal entity. However, many providers have suggested that other interpretations are possible as well, for example:

- Health care entities that have a contractual relationship are related health care entities;
- Health care entities that share employees are related health care entities; and
- Health care entities that share some common ownership, even if not owned and operated by the same legal entity, are related health care entities.

Again, the inability for providers to clearly agree on the definition of “related health care entity,” means that they cannot clearly agree on when patient consent is required for the release of patients’ health information.

Responsibility and Liability for Obtaining Patient Consent

This section begins to highlight the overlap between two of the issues identified as overarching privacy and security issues – Minnesota’s patient consent requirements and liability concerns. It also demonstrates how health care providers’ consideration of organizational risk and their efforts to minimize liability for inappropriate disclosure of patient data can result in practices that impede the real-time, electronic exchange of health information.

Minnesota’s patient consent requirements place all responsibility and liability for the appropriate release of patients’ health records on the health care provider releasing records and places no responsibility on health care providers requesting the records. A health information exchange generally expects all of the actors to have responsibilities for ensuring the appropriateness of the exchange of patient information. Therefore, it is reasonable to ask:

- How do Minnesota’s patient consent requirements impact the development and implementation of health information exchanges?
- How does defining Minnesota’s patient consent requirements in terms of “the release of health records” rather than “the exchange of health records” impact the use and implementation of patient consent in a health information exchange?
- What issues would Minnesota need to address to redefine Minnesota’s patient consent requirements in terms of the exchange of health records?

To protect their patients’ privacy and to minimize their liability, health care providers have developed and implemented many policies and practices associated with obtaining, documenting, and validating patient

consent for the release of health records. Many organizations' policies and procedures were developed to reduce liability concerns rather than to facilitate the rapid exchange of information. Consequently, most policies and practices related to patient consent require extensive human activity, oversight, and involvement.

Consider how the consent requirements affect providers' practices. First, health care providers asked to disclose health records do not rely on the requestor's representations about having obtained the patient's consent for the requested information. Rather, the disclosing provider requires a hard copy of the patient's consent as documentation. Organizations' unwillingness/inability to rely on the requestor's representation of having obtained valid patient consent means that no health information will be exchanged until the disclosing provider completes their review of the documentation. Even if the requesting provider is willing to certify that they have appropriate and valid patient consent, there is no mechanism to avoid the remaining steps in the discloser's process.

After receiving the hard copy of the consent, the disclosing provider manually reviews the form to ensure that it is valid and meets all of the disclosing providers' requirements, which may be even more stringent than Minnesota law. A provider's initial review to validate a patient's consent may address:

- Does the consent meet the requirements of Minnesota law? At a minimum, the Minnesota requirements are a written, signed and dated document. Presumably, the requirements must also include: what records are to be disclosed, who is to disclose the records, and who is to receive the records.
- Does the consent contain all of the HIPAA-required elements for a valid authorization? Some providers require these elements for all authorizations/consents, while others only require the elements for authorizations needed under the HIPAA Privacy regulations.
- Does the consent appropriately specify the data to be disclosed and comply with other relevant consent requirements? For example, does the consent specifically identify substance abuse treatment records when such records are requested?
- Is the consent in effect and not expired?

If the consent/authorization is missing elements or otherwise determined to be invalid, the patient's health information will not be released and a new, corrected consent will need to be obtained. If the provider determines that the patient's consent is valid, the provider will next determine if the patient's consent is sufficient to provide the requested information. This may not be a straightforward process.

The consent process gives patients control over what information is disclosed, but different patients have different concerns. Therefore, the description of the data to be disclosed can vary significantly patient by patient. Operationally, this flexibility afforded to patients through the consent process can be problematic. The description of information to be disclosed may not provide sufficient detail to ascertain the patient's desires, particularly in situations where the patient explicitly consents to the release of one type of information but also explicitly prohibits the release of another type. For example, a patient consents to the release of medication history but not mental health information. If that patient takes an anti-depressant, has the patient given, or not given, consent to release the information about the anti-depressant medication?

A final difficulty facing the releasing provider is that the determinations about the patient's wishes often need to be made in the absence of the patient. A health care provider will often request a patient's health records as the result of a recent patient visit. It is the requesting provider's current, active treatment relationship with the patient that is generating the request for health records from the disclosing provider. The disclosing provider may not have an active treatment relationship with the patient, or even have seen the patient for an extended period of time. Yet, it is the disclosing provider that requires the patient's written consent and

determines if information being requested is consistent with the consent. It would seem logical that this task is more easily completed by the provider who has a current treatment relationship with the patient because they are in the best position to communicate to the patient about what information is needed, why it is needed, and the consequences of not having the information.

With a better understanding of how providers respond operationally to Minnesota's patient consent requirements, we can reexamine the three questions at the beginning of the section:

- **How do Minnesota's patient consent requirements impact the development and implementation of health information exchanges?**

Minnesota's patient consent requirements place all responsibility for the appropriateness of releasing health records on the disclosing provider. Providers' policies and practices to execute the consent requirements are time consuming and require significant human intervention. Health information exchanges are intended to facilitate the real-time (automated) exchange of patients' health information to ensure that providers have all necessary information for patient care. It seems impossible to incorporate providers' current consent practices into a health information exchange and achieve real-time sharing of information. Similarly, it seems impossible to eliminate Minnesota's patient consent requirements without negatively impacting patients' privacy protections. Therefore, unless Minnesota's patient consent requirements are somehow modified to maintain consent and to permit the real-time exchange and validation of patient consent, the development and implementation of health information exchanges will be impeded.

- **How does defining Minnesota's patient consent requirements in terms of "the release of health records" rather than "the exchange of health records" impact the use and implementation of patient consent in a health information exchange?**

By defining Minnesota's patient consent requirements in terms of "the release of health records" rather than "the exchange of health records", Minnesota law is silent on the responsibilities and liabilities of a health care provider requesting health records. That silence means that a provider requesting health information bears no responsibility for ensuring that the exchange of information is appropriate and done with patient consent.

It is unfortunate that the requesting provider does not have clearly defined responsibilities for obtaining and validating the patient consent to exchange health information, because the requesting provider may be better situated to perform some of the responsibilities currently being performed by the disclosing provider. It is the requesting provider that:

- is most likely to have a current treatment relationship with the patient;
- is most likely to have face-to-face interaction with the patient and the ability to address consent related issues; and
- is in the best position to help the patient understand what information is needed, why it is needed, the consequences of not having the information, and the consent required to obtain the information.

Thus, defining Minnesota's patient consent requirements in terms of "the release of health records" ignores a vital resource that may help enable providers to obtain and validate patient consent in real time.

- **What issues would Minnesota need to address to redefine Minnesota's patient consent requirements in terms of the exchange of health records?**

The previous questions raised concerns that the development and implementation of health information exchanges will be impeded unless patient consent requirements are somehow modified

to maintain consent and facilitate the real-time sharing of patient data. The questions identified the requesting provider as an under-utilized resource capable of playing a more significant role in implementing patient consent.

To more fully utilize the requesting provider, Minnesota law would need to provide a framework and mechanism to transfer/share current responsibilities and liability from the disclosing provider to the requesting provider. For example, Minnesota law could permit health records to be exchanged when a requesting provider obtains the patient's consent and then communicates to the disclosing provider that it has appropriate patient consent for the information being requested. There may be multiple mechanisms to transfer the responsibilities and liability between the disclosing and requesting provider, but Minnesota law would minimally need to address:

- When a provider disclosing health records may rely on a requesting provider's representation of having obtained patient consent for the requested health records;
- The responsibilities of a provider requesting health records when a request for health records is based on the representation of having obtained appropriate patient consent;
- The liability of a disclosing provider for having released records based on a requesting provider's misrepresentations of having obtained patient consent; and
- The liability of a requesting provider for misrepresenting that the provider had obtained patient consent when requesting health records.

OPERATIONAL DIFFICULTIES IN IMPLEMENTING ELECTRONIC ACCESS TO PATIENT INFORMATION

As Variations Work Group members first considered the scenarios in Appendix C and then various models of health information exchange, they repeatedly identified a set of security concerns related to their ability to electronically connect and exchange information with other organizations. Most of the Work Group members' organizations are only beginning the process of electronic health information exchange; however, they have already encountered a number of security issues that can impact the privacy of patients' data. Many organizations are developing health information exchange in one-to-one relationships with other health care organizations. In doing so, a number of organizations observed that a number of the solutions being used to address privacy and security issues for information exchanged between two organizations cannot be easily replicated as effective solutions for exchanging information broadly across many organizations.

This section of the report identifies a set of interconnected security problems that must be addressed concurrently to successfully implement a health information exchange. To give external health care providers appropriate access to electronic health records and patient data, organizations need to address four security topics:

- Mechanisms to establish and maintain a list of individuals authorized to access patient data;
- Methods to authenticate authorized individuals who access patient data;
- Information access controls – within information systems and through coordinated organizational policies – to limit authorized individuals' access to those patient data appropriate for the individual's functions and needs; and
- Mechanisms for coordinated auditing across organizations to identify authorized individuals who inappropriately access health information.

This set of issues is significant because health care organizations have not generally been able to adequately address all four topics across organizations, and as a result, are unwilling to place their patient's health information at risk in a health information exchange.

Establishing and Maintaining a List Authorized Individuals

The first issue facing organizations in a health information exchange is who should be authorized to access the organizations' electronic health records or some portion thereof (e.g., provider portal). In thinking about this issue, the Work Group initially restricted its discussion to the situation of two organizations trying to develop a health information exchange. The two organizations can usually identify conceptually who needs to be authorized to access health information. For example, if the organizations' emergency departments are trying to exchange patient information, the people needing access to the health records are the emergency department physicians and nurses. The difficult task is maintaining and managing the list of authorized individuals, particularly as new employees are hired, as existing employees leave, and as employees change positions or responsibilities. Additionally, some changes to the list of individuals authorized to access health information need to be addressed immediately. For example, when employees are terminated, their access to health information also needs to be terminated. Hence, the organizations need a mechanism to quickly exchange information between their human resource departments. They also need a mechanism to use the information to add and remove authorized users in a timely fashion.

When a health information exchange involves more than two organizations, the task of maintaining authorized individuals becomes even more difficult to manage. Each organization needs to exchange information with every other organization's human resource department, or a central entity needs to exchange information with every organization and manage the list of authorized users. Work Group members are concerned that connecting the organizations' human resource departments and ensuring the timely exchange of information to manage authorized users is a task that rapidly grows in complexity as the number of organizations increases. Because organizations have not traditionally needed to exchange this information, especially in real time, the methods and mechanisms to do so are untested. Consequently, organizations worry about their ability to adequately manage the list of authorized users.

Authenticating Authorized Individuals Accessing Health Information

After organizations determine who should be authorized to access their electronic health records, they need to address the issue of how external users will be authenticated when accessing health records. Many organizations have experience in providing employees remote access to health records and that experience guides their thinking in authenticating external, authorized individuals. Currently, most organizations use two-factor authentication when providing remote access to health records. That is, remote users verify their identity with both a password and a security fob that produces a new 5-7 digit random number every 30-60 seconds. To remotely access health records, a user must correctly enter their user ID and both pieces of authenticating information. Because the security fob displays a new random number every 30-60 seconds, the system is considered very secure.

From a security viewpoint, two-factor authentication means the system is secure with good user authentication. However, from a user's viewpoint, the system can be cumbersome to use, because individuals may have multiple user IDs and passwords that change frequently. Additionally, individuals need to carry multiple security fobs for the different systems they are authorized to access. As the number of organizations giving health care providers access to their electronic health record increases, so do the number of IDs, passwords, and security fobs. The need to manage all of these security measures places a burden on the individual health care provider that acts as a barrier to accessing patient information. Hence, this security issue's solution is very difficult to integrate into the normal workflow of health care providers.

One way to address the proliferation of user IDs, passwords, and security fobs is to have a central entity that is responsible for authenticating the user and then permitting access to multiple organizations' health records. Minnesota has a health information exchange that is currently researching and testing centralized

authentication, or single-site sign on. We will follow the progress of these efforts as our project continues to see if their experience can benefit other organizations looking to form a health information exchange. Similarly, efforts around the concept of federated identity management may offer solutions to address these issues and we will examine these efforts as the project continues.

Access Controls to Appropriately Limit Access to Patient Data

The third issue facing organizations in a health information exchange is what information should authorized individuals be permitted to access and what controls can be established to restrict or limit individuals' access to data. The Variations Work Group stated that ideally health care providers should only have access to information for patients with whom they have a treatment relationship and then only to the health information relevant to the treatment being provided. However, it is nearly impossible to set information system controls that enforce the ideal level of access. Thus, organizations are required to establish information access controls through organizational policies and rely on individuals' compliance with the policies to appropriately restrict access.

The Variations Work Group identified a number of practical difficulties in setting information system controls that automatically enforce appropriate access. First an organization needs to know which patients and providers have, or will have, treatment relationships. Information system controls also need to be able to adjust as patient/provider relationships change. It may be difficult to know in advance which patients and providers will have a treatment relationship, particularly when patients have the ability to choose various providers or clinics within a health care network. Even within a single visit, the list of providers that have a treatment relationship with the patient may change based on laboratory tests, physician diagnoses, consults with other providers, and other treatment activities. Consequently, it is not feasible to create a table specifying which providers should have access to particular patients' records. Even if such a table were possible, maintaining the table would be an impossible administrative task.

Another practical difficulty in setting information system controls is determining what information should be available to a provider treating a patient. Without advance knowledge of a patient's condition and treatment needs, it is nearly impossible to specify what information is relevant to treating the patient. Consequently, if it is not possible to specify what information may be relevant, it is not possible to set system controls that restrict access to only necessary information. A third practical difficulty is that if the controls are set too stringently, they may interfere with the delivery of patient care. When a health care provider is unable to access information necessary to treat the patient, either the patient will receive suboptimal care, tests will need to be unnecessarily repeated, or the patient's care will be delayed as the provider works to access the needed information. Hence, information system controls can be difficult to establish, nearly impossible to maintain, and if set incorrectly, interfere with patient care.

An example of the limitations of information system controls can be seen in organizations' current use of role-based access to health records. Role-based access allows organizations to restrict individuals' access to only that patient information relevant for the employees' jobs. However, role-based access enforced through information system controls usually only limits what information may be accessed. It does not usually limit which patients' data are accessible. All Work Group members' organizations use role-based access, but such access still allows authorized individuals to inappropriately access health information.

To address the inherent limitations of information system controls and role-based access, organizations develop policies that set appropriate limits on individuals' access to health information. However unlike automated controls, policies require individuals' compliance to be effective. To achieve and ensure individuals' compliance with policies that restrict access to appropriate data, organizations do three things:

1. Conduct training programs that assist employees in understanding and applying the policies;
2. Deploy mechanisms to monitor and audit employees' compliance with the policies; and

3. Set sanctions for disciplining employees found to be violating the policies.

Most Work Group members have experience with these three activities because many have needed to develop and implement such policies as they have deployed electronic health records within their organizations.

All Variation Work Group members' organizations provide their employees training in the appropriate use of electronic health records. While such training tends to focus on how to use and navigate the electronic health record, all organizations' training includes privacy and security issues related to the use of electronic health records. The questions that would need to be addressed in training about access control policies highlights the Work Group's concerns with using organizational policies to appropriately restrict access in a health information exchange. These concerns are captured in the following unresolved questions:

- When there are variations in when and how organizations' policies restrict access to health information, how will those differences be resolved within a health information exchange?
- Will organizations need to have different access policies for each health information exchange?
- When the access policies for a health information exchange are different than an organization's usual internal policies, what new training requirements will organizations need to address?
- How many different access policies should employees be expected to understand and apply?

The Work Group is also concerned about the ability to develop and deploy appropriate mechanisms to monitor and audit individuals' compliance with access control policies. Many of these concerns are developed in the next section, although an overview of the issues is presented here. In general, organizations have the ability to monitor and log which authorized individuals have accessed their electronic health records and what information was accessed. However, the determination of whether or not the information was appropriately accessed requires knowing if there was a legitimate need to access the information. The audit log does not provide information to determine if there was a legitimate need for the data. The legitimate need to access the data must be determined by looking at other data sources that address questions such as:

- Was the patient being seen when the data was accessed?
- Why was the patient being seen?
- Who was involved in the patient's treatment?

Organizations involved in a health information exchange need to develop mechanisms to coordinate the auditing of information accessed across the various organizations participating in a health information exchange. Yet, many organizations remain cautious in developing mechanisms for coordinated auditing. All organizations are responsible for maintaining the privacy and confidentiality of their patients' health information. A health information exchange's need for coordinated auditing means that organizations must rely on external entities to assist in monitoring individuals' compliance with access control policies designed to protect their patients' privacy and confidentiality. This reliance on external entities raises many liability concerns for organizations and explains their caution in developing coordinated auditing mechanisms.

Another area of concern in using policies to appropriately restrict access to health information is the application of sanctions to external authorized individuals. To illustrate this concern, the Work Group considered a simple health information exchange between Organization A and Organization B. If the two organizations have different sanction policies, which organization's sanctions should be applied to an employee from Organization A for inappropriately accessing Organization B's electronic health record? What happens if Organizations A and B disagree about how sanctions should be applied to a particular situation? Disciplinary sanctions are important tools in ensuring compliance with policies and by extension for ensuring the privacy and confidentiality of health information. Therefore, organizations are concerned about their

ability to adequately protect the privacy of health information when their ability to apply sanctions is impaired/limited.

Auditing Authorized Individuals Access to Patient Data

As described in the last section, monitoring and auditing authorized individuals' access to patients' health information is a critical step in ensuring compliance with organizational policies designed to protect the privacy and confidentiality of health information. Yet, the Work Group questioned the overall effectiveness of auditing and monitoring and was apprehensive about the role of auditing in protecting the privacy and confidentiality of health information. The Work Group noted that auditing was really a tool of last resort. That is, auditing may be able to identify situations where health information has been inappropriately accessed, but does nothing to stop the inappropriate access before it happens.

Variations Work Group members were able to use their organizations' internal experiences with monitoring and auditing to describe their concerns of using the same tools in a health information exchange. Organizations' first concern is the large volume of data that is generated as part of the auditing process. Auditing logs can quickly grow to an unmanageable size, which creates a problem for trying to store and review the logs. Additionally, nearly all of the information in an audit log is evidence of appropriate behavior and the appropriate accessing of health information. Consequently, the problem becomes one of trying to find a needle in a haystack. That is, an audit log may have tens of thousands of entries, yet a very small number of these may be indicative of a problem of inappropriate access to health information. There needs to be automated/non-manual tools and techniques to sort through the large volume of data and separate the appropriate access from the inappropriate. The Work Group pointed out that these vital tools are generally lacking.

Because organizations lack effective tools to analyze audit logs, they rely on other methods. Most organizations perform complaint-based auditing and VIP auditing. Complaint-based auditing is a review and analysis of the audit logs done in response to complaints or suspicions of inappropriate behavior. Complaint-based auditing allows an organization to focus its analysis on a particular individual or incident; however, it requires a complaint or suspicion of inappropriate behavior to initiate the review and analysis. When an individual inappropriately accesses health information in a manner that does not lead to a complaint or other suspicions, the inappropriate behavior is likely to go undetected. VIP auditing is a review and analysis of all access to the health records of individuals likely to attract attention (e.g., celebrities, public figures, employees, etc.). VIP auditing is useful and effective because it reviews the audit logs for inappropriate access to those records most likely to be inappropriately accessed, but it is a resource intensive review that could not be done for all records.

One of the reasons that organizations find it particularly difficult to review and analyze audit logs is that audit logs only provide details about information and records accessed and not the legitimacy of the access. Determining the legitimacy of individuals' access to information requires additional knowledge from outside of the audit logs (e.g., patients' scheduled visits or physicians consulting on patients' cases). Organizations generally do not have intelligent tools capable of automatically collecting, organizing, and analyzing the information necessary to assess the appropriateness of individuals' access to health information. The process of collecting and analyzing these data is still a manual, resource-intensive activity that requires human intervention. Consequently, auditing may be effective for verifying suspected inappropriate access and for identifying the most egregious cases of inappropriate access, but it is not effective as a general tool in identifying all cases of inappropriate access.

Given their internal experiences with auditing access to electronic health records, Work Group members were even more concerned about monitoring and auditing access to records in a health information exchange. Within their organizations, they usually have the information necessary to determine if any particular access to information was appropriate, even if it is a resource-intensive, manual process. When an external individual accesses their health records, organizations usually do not have the information necessary to

determine if the access is legitimate and must rely on others participating in the health information exchange to verify the legitimacy of the access. Hence significant collaboration and coordination will need to occur between organizations in a health information exchange for auditing to be effective in protecting the privacy and confidentiality of health information. As with other issues in this section, this type of collaboration and coordination has not traditionally been done. Consequently, organizations are concerned about:

- How to feasibly incorporate these new cross-organizational tasks into their daily operations; and
- The risks and legal liabilities these new activities will create for their organizations.

Summary of Operational Concerns

This section of the report identified a set of interconnected security problems that must be addressed concurrently to successfully implement a health information exchange. Addressing the security issues requires organizations to collaborate and coordinate activities in new and untested ways. The uncertainty associated with trying to address these security issues raises a number of new risks and liabilities for organizations. These security concerns create barriers to the electronic exchange of health information that can be summarized as organizations' difficulty or inability in satisfactorily answering the following questions:

- Which individuals from other organizations within the health information exchange should be authorized to access my organization's electronic health records?
- How will the organizations exchange the information needed to maintain the list of individuals authorized to access health records?
- What mechanisms will be deployed to rapidly respond to changes in the list of authorized users as new employees are hired, as existing employees leave, and as employees change positions or responsibilities?
- How will external individuals be authenticated?
- How will our organization address the cumbersomeness of the ever-increasing number of user IDs, passwords, and security fobs providers are required to manage to access health information?
- What can be done to ensure that security measures designed to protect the privacy of patients' information does not interfere with providers' abilities to treat patients?
- What mechanisms and tools can be deployed to limit providers' access to patient information to those patients with whom the provider has a treatment relationship?
- Can organizational policies to control access to health information be effective?
- What training will employees need to understand and appropriately apply access control policies?
- How will differences in organizations' access control policies be resolved in a health information exchange?
- How many different access control policies should employees be expected to understand and apply?
- What mechanisms should organizations in a health information exchange use to coordinate their monitoring and auditing of access to health records?
- How should sanctions be applied across organizations when individuals inappropriately access information within a health information exchange?

- What happens if organizations in a health information exchange disagree about when and how to apply sanctions to an individual for inappropriately accessing information through a health information exchange?
- What tools and techniques can be deployed to manage the large volume of data generated in auditing logs?
- How can audit logs data be combined with other data sources to verify the legitimacy of data access?
- What needs to be done to minimize our organization's liability when they must rely on other organizations to audit and verify the legitimacy of individuals accessing health records?

LIABILITY CONCERNS AS A BARRIER TO THE EXCHANGE OF HEALTH INFORMATION

One of the reasons that health care organizations are particularly concerned with privacy and security issues is that inappropriate or unauthorized disclosures of health information can be a source of significant liability. Some of the sources of liability include:

- The Office of Civil Rights at the U.S. Department of Health and Human Services, which enforces the HIPAA Privacy regulations;
- The United States Attorney General who enforces federal regulations governing chemical dependency treatment records;
- State regulators who conduct reviews based on licensure;
- State licensing boards that license individual providers such as physicians, nurses, chiropractors and others. Minnesota Statutes, section 144.335, subdivision 6 specifically provides that inappropriate use and/or disclosure of patient health information can be the basis for disciplinary action against a license holder;
- Litigation by patients or their representatives under Minnesota Statutes § 144.335, subdivision 3a, paragraph (e); and
- Negative publicity through any type of news media.

While all sources of liability are of concern to health care organizations, negative publicity is a particularly significant source, because of the resulting damage to the "brand" of a health care organization. There is no way to "repair" a brand, other than the passage of time. Such liability is difficult to measure and difficult to counteract. Negative publicity can also result in the loss of patient confidence, a reduction in the number of payers willing to do business with a provider, and a reduction in the value of goodwill and reputation that the provider has developed over time. There is no insurance to return the organization to their position before the problem and no way to write contractual provisions to prevent damage to brand. Recovery from each of these types of liability is difficult and hard won.

Because liability for inappropriate or unauthorized disclosures of health information can result in significant loss that is not easily remedied, health care organizations are cautious in their approach to exchanging data. When health care organizations have liability concerns about the exchange of information, the exchange will generally not occur. They want to be confident that any mechanism for exchanging health information has adequately addressed privacy/security issues and minimizes their organization's liability.

Previous sections of the report highlighted how liability concerns are manifest in patient consent. Organizations minimize potential liability by systematically reviewing the consent for all the required elements and being cautious in its disclosures in response to the consent. Any questions or concerns are resolved through nondisclosure. The consent processes are time consuming and require significant human intervention, but significantly reduce an organization's liability.

Therefore, this barrier is important, in that, it explains why the most significant barriers are those issues for which organizations have not been able to find any sufficient mechanisms to address privacy and security concerns. Health care organizations are able and willing to modify their business practices to facilitate the exchange of information when there are multiple practices that minimize the organizations' liability. In contrast, organizations are unwilling to exchange data when they are unable to find business practices that sufficiently control their liability.

This barrier also helps to explain why the other two overarching privacy and security issues are considered the most significant impediments to the development and implementation of health information exchanges. In general, organizations have not found any good practices for complying with Minnesota's patient consent requirements that both facilitate real-time exchange of information and do not create unacceptable levels of liability. Likewise, the practices required to grant external organizations access to patients' data (e.g., authorizing users and auditing access) generally are untested, complex activities that create many liabilities for organizations.

While it may not be feasible or even desirable, to eliminate this barrier by eliminating organizations' liability for inappropriate or unauthorized disclosures of health information, this barrier should cause us to:

- Assess if liability is appropriately distributed across all of the actors involved in the exchange of health information; and
- Focus our efforts on those privacy and security issues creating the greatest liability for organizations, because those issues most impede the advancement of health information exchanges.

CONCLUSIONS

The privacy and security barriers to the electronic exchange of health information identified in this report are a mix of legal, technological, and organizational issues that need to be addressed through a variety of means. The Work Groups' analysis of the barriers to be addressed to encourage the electronic exchange of health information can be summarized as follows:

- Patient consent requirements must be clarified.
- Technology must be developed and organizational policies changed to address difficulties in providing, limiting and monitoring external organizations' access to patient data.
- A legal, technological and organizational framework must be developed to address organizations' liability concerns that are operationally feasible for ensuring the privacy, security, and confidentiality of patients' data.

These barriers may be difficult to reduce or eliminate. However, prioritizing action around these privacy and security issues is necessary to facilitate development and implementation of health information exchanges. Finding workable solutions to these barriers will improve the privacy and confidentiality of patients' data and reduce the liability concerns that impede health care organizations' willingness to engage in the electronic exchange of information.