

INTERIM REPORT ON SOLUTIONS TO 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

January 16, 2007



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 Group and Subgroup meetings. These participants' input and analysis has been critical to accomplishing the goals of the project and in identifying, analyzing, and documenting the solutions for 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
Executive Summary	2
Background and Purpose	4
The Minnesota e-Health Initiative	4
The Minnesota Privacy and Security Project	5
Health Information Exchange - Concepts and Terminology	6
Project Methodology	9
Project Structure	9
Project Activities – Phase I	11
Project Activities – Phase II	12
Solutions and Options for Addressing Privacy and Security	
Barriers to the Electronic Exchange of Health Information	15
Introduction	15
Overview of Barriers to the Electronic Exchange of Patients’ Health Information Caused by Minnesota’s Patient Consent Requirements	16
Analysis of Solutions and Options for Addressing Barriers Caused by Minnesota’s Patient Consent Requirements	17
Informed Consent and Enforcement	42
Overview of Authorization, Authentication, Access Control, and Auditing Issues	43
General Principles for Authorizing and Authenticating Individuals, Setting Access Controls, and Auditing in a Health Information Exchange	44
Expanded Discussion and Analysis of General Principles	47
Conclusions	58
Appendix A Security Terms and Definitions	58
Appendix B Health Care Security Standards and Definitions	58

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 critical issues related to the security and confidentiality of health information and patient privacy requirements in this new era of electronic health information exchange. The Minnesota Privacy and Security Project (MPSP) is a first step in fulfilling that responsibility.

Health industry stakeholder and consumer involvement in the MPSP is critical to ensuring that project 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 website at: <http://www.health.state.mn.us/e-health/mpsp/>

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." The Minnesota e-Health Advisory Committee serves as the steering committee for the purposes of the HISPC contract.

Under the Minnesota e-Health Advisory Committee's direction, the MPSP conducted a systematic and comprehensive review of current laws and practices to identify the most significant privacy and security barriers facing organizations in implementing the electronic exchange of health information. At the end of the project's first phase in October 2006, the MPSP issued a report titled, "*Privacy and Security Barriers to the Electronic Exchange of Health Information*." That report identified the two most significant privacy and security issues that must be solved to advance the appropriate electronic exchange of health information as:

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 that 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 no 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;

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

- 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.

Currently, the second phase of the MPSP has brought together a Solutions and Implementation Plans Work Group to develop solutions to eliminate or reduce these two privacy and security barriers while preserving and strengthening patient privacy protections. The Solutions and Implementation Plans Work Group formed two subgroups to address each of the barriers individually.

The Patient Consent Subgroup examined differences between health care providers regarding “when” and “how” patient consent is required to exchange patients' health information. This Subgroup identified a number of potential solutions – including advantages and disadvantages for each solution – to address nine specific patient consent issues related to:

- Undefined terms and ambiguous concepts that are used in Minnesota's patient consent requirements in Minnesota Statutes § 144.335;
- Difficulties in determining the appropriate application of Minnesota's patient consent requirements to concepts in the electronic exchange of health information that do not have an analogous concept in a paper-based exchange; and
- The need to update Minnesota's patient consent requirements to allow mechanisms that facilitate the electronic exchange of patients' information while respecting the patients' ability and wishes for controlling their information

The Authorization, Authentication, Access Control and Auditing Subgroup (4A Subgroup) developed a set of 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange. These principles provide Minnesota health care organizations a foundation and framework for the continued development of Health Information Exchanges and can guide organizations' decision making in forming and implementing Health Information Exchanges. The general principles form a “conceptual solution” that was developed to be:

- Independent of a particular Health Information Exchange architecture;
- Flexible enough to adapt to changes in information technology;
- Consistent with national standards currently under development; and
- Capable of being refined and more finely detailed as health care organizations gain experience in implementing the electronic exchange of health information.

This second report of the Minnesota Privacy and Security Project is an interim report that details the work of the Patient Consent Subgroup and the 4A Subgroup to develop solutions that eliminate or reduce the two most significant privacy and security barriers to the electronic exchange of health information. In February, 2007, the on-going work of the project and the two Subgroups will result in another interim report that identifies and describes mechanisms and plans to implement the solutions outlined in this report. A final Minnesota Privacy and Security Project report that combines all of the three project reports into a final, comprehensive report is anticipated in April, 2007.

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 information³. 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.

³ 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 analyzed 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 the 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 the electronic exchange of health information;
- 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 the electronic exchange of health information and privacy/security issues contribute to and learn from national efforts.

This document is the second report issued by the MPSP and builds on the first report titled, "*Privacy and Security Barriers to the Electronic Exchange of Health Information*⁴." The first report details the two most

⁴ A copy of the report is available at: <http://www.health.state.mn.us/e-health/mpsp/index.html>

significant and overarching privacy and security issues that must be solved to advance the appropriate electronic exchange of health information in Minnesota, specifically:

- Implementation of Minnesota's patient consent requirements within a Health Information Exchange; and
- Operational difficulties in first providing, and then limiting and monitoring external organizations' electronic access to patient data.

This report documents the MPSP's efforts to develop solutions to address these barriers and to advance the development and use of interoperable health information technology in Minnesota.

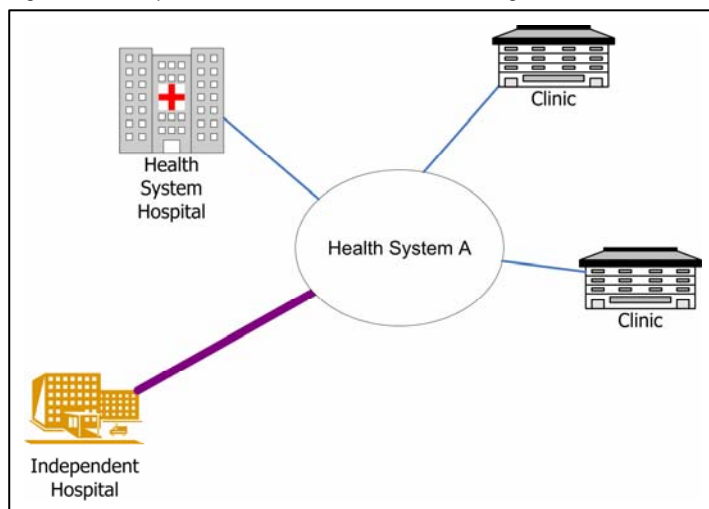
HEALTH INFORMATION EXCHANGE - CONCEPTS AND TERMINOLOGY

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"**.

Figure 1 – A Simple Model of Health Information Exchange



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

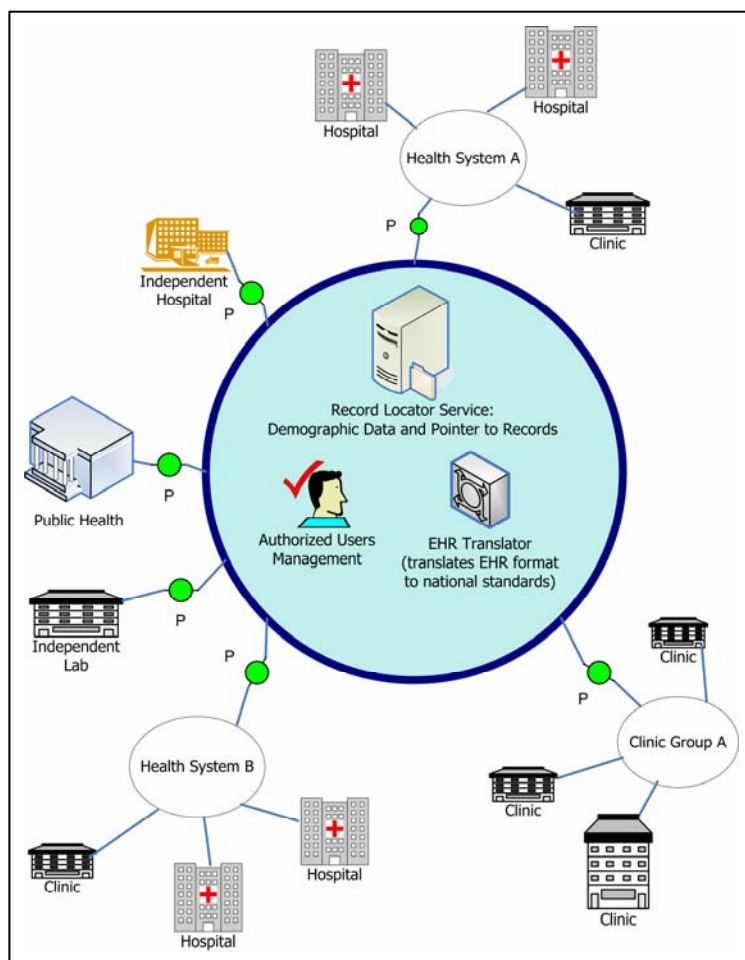
⁵ This definition is an adaptation the e-Health Initiative's definition. See <http://www.ehealthinitiative.org/>

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
 - 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:
 - Medical history
 - Medication history
 - 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.

There are portions of this report that use a number of information system security terms, particularly those portions that address the operational difficulties in first providing, and then limiting and monitoring external organizations' electronic access to patient data. Although Appendix A, *Security Terms and Definitions*, provides a more complete listing of security terms and definitions, it is important to highlight four terms that are used frequently in the report:

- **Authorization** refers to the official management decision to permit access to information systems and patients' health information.
- **Authentication** refers to the basic processes and mechanisms for validating that someone is who they claim to be. The authentication process is usually based on one or more of the following factors:
 - Something a person knows (e.g., account/user name, password, PIN, ID number);
 - Something a person has (e.g., token, bank card, driver's license, passport); or
 - Something a person is (e.g., biometrics, fingerprint, retina, DNA, signature).
- **Access Controls** refers to the policies, procedures, processes, and mechanisms for granting or denying specific requests to obtain and use patients' health information through information systems.
- **Auditing** refers to the review and examination of records and activities to assess the adequacy of systems controls for ensuring compliance with established policies and operational procedures for appropriately accessing patients' health information.

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

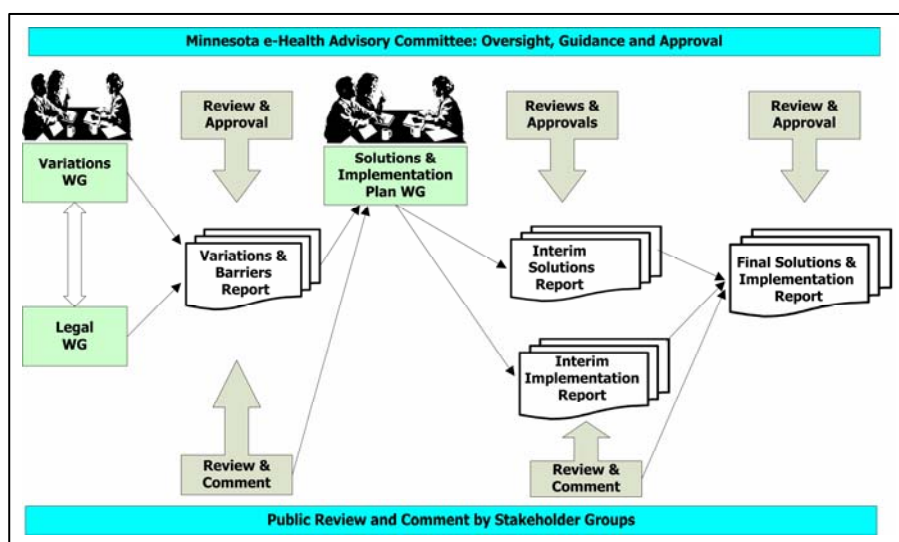
PROJECT METHODOLOGY

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



- 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. 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 Health Information Exchanges.

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. 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 consists of individuals representing consumers, health systems, health plans, hospitals, public health agencies, and other organizations involved in the exchange of health information. The individuals provided 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 has two responsibilities:

- Develop solutions to eliminate or reduce the most significant privacy and security barriers impeding the electronic exchange of health information, while preserving and strengthening patient privacy protections; and
- Create action plans to implement the solutions identified and developed in response to the privacy and security barriers identified in this report.

To achieve these responsibilities the Solutions and Implementation Plans Work Group formed two subgroups: 1) Patient Consent Subgroup; and 2) Authorization, Authentication, Access Control and Auditing Subgroup

(aka the 4A Subgroup). Each of the Subgroups addressed one of the two overarching privacy and security issues identified in the first project report.

PROJECT ACTIVITIES – PHASE I

The first phase of this project occurred between June, 2006 and October, 2006. This phase of the project was a determination, assessment, and evaluation of the most significant privacy and security barriers to the electronic exchange of health information in Minnesota. This first portion of the project was conducted by the Variations Work Group and the Legal Work Group and addressed the following three areas.

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.

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 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 privacy and security barriers to the electronic exchange of health information based on the situations described in each scenario.

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 issues, 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.

PROJECT ACTIVITIES – PHASE II

The second phase of this project is an on-going activity that began in October, 2006. This phase of the project builds on the work completed by the Variations Work Group and the Legal Work Group in the first phase of the project. This second portion of the project is being conducted by the two subgroups of the Solutions and Implementation Plans Work Group and is addressing the following areas.

Addressing Issues Related to Minnesota's Patient Consent Requirements

A number of patient consent issues must be addressed to advance the automated, real-time electronic exchange of health information through a Health Information Exchange. These issues generally revolve around differences between health care providers regarding "when" and "how" patient consent is required to exchange patients' health information. These differences and issues generally result from:

- Undefined terms and ambiguous concepts that are used in Minnesota's patient consent requirements in Minnesota Statutes § 144.335 (e.g., "Health Record" being undefined);
- Difficulties in determining the appropriate application of Minnesota's patient consent requirements to concepts in the electronic exchange of health information that do not have an analogous concept in a paper-based exchange (e.g., record locator service); and

- The need to update Minnesota's patient consent requirements to allow mechanisms that facilitate the electronic exchange of patients' information while respecting the patients' ability and wishes for controlling their information (e.g., the ability to rely on another provider's representation of having obtained patient consent to exchange health information).

The Patient Consent Subgroup discussed and analyzed potential solutions to these issues over the course of seven meetings. The two-hour meetings were held between October 18, 2006 and January 3, 2007. The discussions focused on identifying solutions and implementation activities that eliminate or reduce barriers to: 1) implementing Minnesota patient consent requirements into electronic exchanges of health information, while maintaining or strengthening patient privacy protections; and 2) ensuring that all parties involved in the electronic exchange of health information share responsibility/liability for the appropriateness of the exchange. Specifically, the Subgroup was charged with:

- Identifying options for adding definitions and clarifications to Minnesota's patient consent requirements, as well as other mechanisms that could facilitate electronic exchange of health information;
- Identifying and documenting the advantages and disadvantages of each option/mechanism;
- Connecting related options/mechanisms into a coherent solution set;
- Documenting any issues or difficulties associated with implementing various options/mechanisms; and
- Finding consensus on options/mechanisms – when possible.

Developing a Framework and Principles for Addressing Key Security Topics

To give external health care providers appropriate access to electronic health records and patient data through a Health Information Exchange, 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 when accessing patient data;
- 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
- Mechanisms for coordinated auditing across organizations to identify authorized individuals who may have inappropriately accessed health information.

The 4A Subgroup addressed these issues over the course of six meetings. The two-hour meetings were held between October 18, 2006 and January 10, 2007. Originally, the 4A Subgroup intended to use a three step model for generating solutions and action plans for addressing these issues. The three steps were to:

- Develop a conceptual solution that describes the characteristics or requirements for a solution to adequately address each of the four issues;
- Identify specific policies, procedures, mechanisms or technologies as options/solutions that met the characteristics or requirements for a solution; and
- Develop action plans to implement the policies, procedures, mechanisms or technologies identified as solutions.

Once the 4A Subgroup began meeting it quickly realized that any specific policies, procedures, mechanisms or technologies that might serve as solutions would be highly dependent on a number of evolving factors that are outside of the Subgroup's control, such as:

- The results, work products, and standards from national groups and projects related to authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange;
- The healthcare industry's on-going experiences with defining and implementing particular architectures and networks of Health Information Exchange;
- Technological changes that provide enhanced ability to implement technology solutions to the issues identified by the 4A Subgroup; and
- The sharing of "best practices" and "lessons learned" as health care organizations participating in Health Information Exchanges gain experience in implementing exchanges.

Therefore, the 4A Subgroup focused its efforts on developing a set of 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange. The 19 Principles are based on five general assumptions about Health Information Exchanges and are intended to serve as general principles that are:

- Independent of particular technologies or specific Health Information Exchange architectures;
- Time invariant so that they are not immediately obsolete; and
- Scalable to accommodate small and large Health Information Exchange models.

In addition to developing 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange, the 4A Subgroup identified recommended resources and experts for further developing and refining the principles to keep pace with the development and implementation of Health Information Exchanges.

SOLUTIONS AND OPTIONS FOR ADDRESSING PRIVACY AND SECURITY BARRIERS TO THE ELECTRONIC EXCHANGE OF HEALTH INFORMATION

INTRODUCTION

In the initial phase of the Minnesota Privacy and Security Project, 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 explored 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 Work Groups' activities revealed that the privacy and security concerns 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 automated, real-time electronic exchange of health information. Additionally, the impediments are the result of organizations not having any fully adequate mechanisms to address the issues/concerns.

The overarching privacy and security issues that must be solved to advance the automated, real-time 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 will benefit the care they deliver and has appropriately addressed privacy/security issues to minimize their organization's liability from inappropriate disclosures of patients' data.

A complete discussion of these three privacy and security issues can be found in the project's first report titled, "*Privacy and Security Barriers to the Electronic Exchange of Health Information.*" A copy of the report is available at: <http://www.health.state.mn.us/e-health/mpsp/>

OVERVIEW OF BARRIERS TO THE ELECTRONIC EXCHANGE OF PATIENTS' HEALTH INFORMATION CAUSED BY MINNESOTA'S PATIENT CONSENT REQUIREMENTS

Minnesota law requires patient consent for the release of health information even if the disclosure is to another health care provider for patient treatment and certain statutory exceptions are not met. Therefore, any Health Information Exchange developed to facilitate the automated, real-time electronic exchange of 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.

In the project's examination of the two fundamental issues, it was clear that providers do not all have the same interpretation of existing 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 and ambiguous concepts lead to fundamentally different interpretations of Minnesota's statutory requirements:

- Health Records - including whether or not patient identifying information is part of a health record
- Medical Emergency
- Related Health Care Entity
- The appropriate application of Minnesota's patient consent requirements to a record locator service, which also requires a common understanding of the concept of a record locator service.
- Current Treatment as referenced in Minnesota Statutes § 144.335, Subdivision 3a, (c)(1)
- The ability of a health care provider to rely on another provider's representation of having obtained patient consent to disclose health records – including mechanisms to transfer/share responsibilities and liability for patient consent between the disclosing and requesting providers

ANALYSIS OF SOLUTIONS AND OPTIONS FOR ADDRESSING BARRIERS CAUSED BY MINNESOTA'S PATIENT CONSENT REQUIREMENTS

This portion of the report examines nine specific patient consent issues that impede health care providers' ability to achieve automated, real-time electronic exchange of health information to deliver patients the best possible health care. For each of the nine issues, the Patient Consent Subgroup identified options to reduce or eliminate the barrier. The Subgroup also described the advantages and disadvantages for each possible solution.

Patient Consent Issue #1

The term "Health Record" is not defined in Minnesota Statutes § 144.335. The patient consent requirements in Minnesota Statutes § 144.335 give patients a measure of control over the disclosure of information contained in their health records. However without an agreed upon definition or understanding of the content of a "health record," patients and health care organizations will not know or concur on what information patients can control. The inability to agree on what information is within patients' control results in disagreement about "when" and "how" patient consent is required to disclose/exchange patients' information. This disagreement has three practical considerations:

1. Different interpretations of the term "Health Record" leads to inconsistencies in patients ability to control their information;
2. Disagreement about what information requires patient consent makes it more difficult to properly automate the exchange of patients' information between health care providers; and

3. Disagreement about the definition of "Health Records" causes disagreement about whether or not patient consent is required to include information about the location of patients' health records in a record locator service.

A number of options were initially discussed to address this issue. The Patient Consent Subgroup considered the following two options in more detail as methods of addressing this issue:

Patient Consent Issue #1 - Option #1.1: Leave the term "Health Record" undefined.

By not defining the term "Health Record," this option continues the current practice in Minnesota. This option was considered because some Patient Consent Subgroup members questioned if the issues that arise from not having a definition are sufficiently serious to warrant developing a definition.

Advantages of Option #1.1

- This option is consistent with current practice in Minnesota and health care organizations would not need to modify their procedures to adapt to a new, explicit definition of the term "Health Record."
- The lack of a definition for the term "Health Record" has not created a significant barrier to the exchange of patients' health information for organizations using paper health records.
- In addition, not defining the term means that no decision needs to be made whether to include or exclude identifying information from the definition.

Disadvantages of Option #1.1

- Without a definition, it will be difficult to achieve consistency across health care organizations on the meaning and scope of the term "Health Records." This lack of consistency on patient consent makes it more difficult to properly automate the exchange of patients' information between health care providers.
- This option does not address inconsistencies in patients' ability to control their information from different interpretations of the term "Health Record."
- This option does not help in determining if identifying information (e.g., name, address, date of birth and other non-clinical data) are part of a health record. This is an important issue because identifying information is needed to help health care providers find the location of patients' health records. Likewise, it is anticipated that this issue will increase in importance as health care organizations form Health Information Exchanges and need to develop mechanisms to locate patients' health records.
- Unless the term "Health Record" is clarified either through definition or other method, there will be on-going disagreement and confusion about how Minnesota's patient consent requirements apply to the creation and use of a record locator service.

Other Issues Related to Option #1.1

- One reason to define the terms "Health Records" and "Identifying Information" is to facilitate the development of a record locator service. Some Patient Consent Subgroup members believe that it is possible to separately define "Record Locator Service" and "Identifying Information" with regard to a RLS, notwithstanding the definition of Health Record under Minnesota Statutes § 144.335. Hence, it may be possible to address the issues related to a record locator service independently of the definition of the term "Health Record."

Patient Consent Issue #1 - Option #1.2: Amending Minnesota Statutes, section 144.335, subdivision 1 by adding:

"Health record" means any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient.

This option is an adaptation of the definition of the term "Health Information" in the HIPAA Privacy Regulations in 45 CFR 160.103.

Advantages of Option #1.2

- Health care organizations currently use this definition as part of their organizations' implementation of the HIPAA Privacy Regulations. Hence, organizations have experience in applying this definition in situations related to patient privacy.
- Health care organizations have general agreement about what information is covered by the term "Health Information" under the HIPAA Privacy Regulations. Therefore, this option would significantly reduce disagreement about what information is included, or contained in a "Health Record."
- Because the HIPAA Privacy Regulations provide some measure of consistency across states, this definition allows Minnesota to be more consistent with other states' definitions of health information and health records.
- Increased consistency and agreement on the meaning of the term "Health Records" supports the real-time, automated electronic exchange of health information, because it helps to clarify "when" and "how" patient consent is needed to exchange patients' information.
- This definition is generally consistent with the definition of "Health Record Information" in Minnesota Statutes 72A.491, Subdivision 10. which reads: *"Health record information" means personal information that: (1) relates to an individual's physical or mental condition, health history, or health treatment; and (2) is obtained from a health professional or health care institution, from the individual, or from the individual's spouse, parent, legal guardian, or other person.*

Disadvantages of Option #1.2

- Although this definition is consistent with HIPAA, the definition may not be consistent with the de facto definition of "Health Records" that health care organizations currently use in applying Minnesota's patient consent requirements.
- Health care organizations may need to modify some of their patient consent processes to ensure that the activities are consistent with this definition. The need to modify organizational processes would represent a cost to health care organizations.
- The broad and inclusive definition of health information in HIPAA is balanced by the ability to disclose health information for the purposes authorized in 45 CFR 164.512. Because Minnesota law does not provide the authority for the same purposes described in 45 CFR 164.512, this option may have unintended consequences affecting the releases authorized in 45 CFR 164.512. For example, under 45 CFR 164.512(2)(i), a health care organization

can release the name, address, date of birth, etc. on a patient for the purposes of identifying or locating a suspect, fugitive, material witness, or missing person. Yet under this option, patient identifying information would be part of the health record and require patient consent to disclose. Thus, Minnesota law would be more stringent than HIPAA and health care organizations would need to follow Minnesota law and not disclose the information. This example is an example of an unintended consequence that is at odds with health care organizations current practices.

- Another example of a potential unintended consequence might be patient directories. Under this option, there is a question of whether or not patient consent would be required prior to using patient's name in a hospital directory. Although this example is an unintended consequence that could be addressed through the appropriate modification of an organization's consent processes.
- Some Patient Consent Subgroup members believe that this definition of "Health Record" is too broad and would cover such information as Customer Service recordings for those patients who call in with an appointment. Although such recordings should be protected from disclosure without the patient's consent, it may not be appropriate or practical for the provider to make that information available to the patient as required in Minnesota Statutes § 144.335, subdivision 2(b).

Other Issues Related to Option #1.2

- Under this definition, the type of information that would be included in a record locator service (e.g., patient identifying information and record location) would be considered a health record. Therefore unless there is a specific exception, patient consent would be needed to populate and/or use a record locator service or other index that facilitates the electronic exchange of patients' health information.

Patient Consent Issue #2:

There is a need to define and introduce the concept and term "Identifying Information" in Minnesota Statutes § 144.335. It would be useful to define a set of non-clinical data elements (e.g., name, date-of-birth) that can be used to uniquely identify patients. Clearly, health care organizations need to be able to distinguish and uniquely identify their patients' records. Similarly when exchanging patients' health information between health care entities, it is critical to be able to uniquely identify patients to ensure that organizations are exchanging information about the same patient. The exchange of health information is only effective if the provider who needs the health information gets the data associated with the patient who needs the care. There are three specific reasons that it might be useful and/or beneficial to define the term "Identifying Information:"

1. It may be useful to exclude non-clinical, patient identifying information from the definition of the term "Health Record." This may help to avoid some of the unintended consequences described in Patient Consent Issue #1 - Option #2;
2. Non-clinical, patient identifying information is critical to the ability to create and use a record locator service in a Health Information Exchange and a definition would clarify what identifying information could be included in the record locator service (see also - Patient Consent Issue #6); and
3. It may be useful to have different consent requirements for patients' non-clinical identifying information and their clinical data.

The Patient Consent Subgroup noted although there are multiple reasons/purposes to define the term "Identifying Information," the definition that is best for one purpose may not be best for another.

The Patient Consent Subgroup considered the following two options as methods of addressing this issue:

Patient Consent Issue #2 - Option #2.1: Amending Minnesota Statutes, section 144.335, subdivision 1 by adding:

"Identifying information" means the patient's name, address, date of birth, gender, parent's or guardian's name regardless of the age of the patient, and other non-clinical data which can be used to uniquely identify a patient.

Advantages of Options #2.1

- This definition provides flexibility in the exact data elements to be used in identifying patients and meets the requirements of a record locator service within a Health Information Exchange.
- Conceptually, the definition allows patients' identifying information to contain sufficient data elements to uniquely identify patients.
- This definition would be consistent with many potential methods of identifying patients across health care organizations.

Disadvantages of Options #2.1

- The inclusion of "other non-clinical data" may be considered too broad and vague. Patients could be concerned that this portion of the definition encompasses too much information.
- Health care providers often do not have, or collect, some of the information listed in the definition (e.g., parent or guardian information for adults).

Other Issues Related to Option #2.1

- A national patient identification number would be helpful in accurately and uniquely identifying patients and linking them to their health records. This definition does not rely on a national patient identifier, but would be consistent with such an identifier.

Patient Consent Issue #2 - Option #2.2: Amending Minnesota Statutes, section 144.335, subdivision 1 by adding:

"Identifying information" means the patient's name, address, date of birth, gender, parent's or guardian's name regardless of the age of the patient, and a number from a government-issued identification card; driver's license or tribal identification card.

Advantages of Option #2.2

- This option provides a more definitive list of data elements that make up patients' identifying information than the list in Option #2.1. The more definitive nature of this list allows patients to better understand what is considered "Identifying Information."
- The data elements that are included in this definition are not generally considered health/medical information.

Disadvantages of Option #2.2

- The inclusion of “a government issued identification card” may be considered too broad and would include government-issued numbers such as a Social Security number. Patients are generally concerned about the use of their Social Security number as a form of identification. Likewise, most health care organizations have stopped using the Social Security number as an identifier in response to feedback from patients. However, this reference could be narrowed to be more selective about the types of government-issued identification.
- This definition may not allow patients’ identifying information to contain sufficient data elements to uniquely identify patients.
- This definition may not have sufficient data elements to be consistent with many potential methods of identifying patients across health care organizations.

Other Issues Related to Option #2.2

- A national patient identification number would be helpful in accurately and uniquely identifying patients and linking them to their health records. This definition does not rely on a national patient identifier, but would be consistent with such an identifier.

Patient Consent Issue #3:

The term “Medical Emergency” is not defined in Minnesota Statutes § 144.335. Patient consent for the release of health records is not currently required in a medical emergency where the provider, due to circumstances, cannot obtain the patient’s consent. Utilizing this exception to Minnesota’s patient consent requirements requires that health care organizations agree when a particular situation is a “medical emergency.” While health care organizations generally agree, there is some variation in organizations’ assessment of situations. Some of the difference may be due to the fact that liability for the inappropriate disclosure of health information rests with the disclosing organization and the disclosing organizations are cautious about disclosing patients’ health information without consent. Adding a definition to Minnesota’s patient consent requirements would help clarify “when” this exception to patient consent is applicable.

A number of options were initially discussed to address this issue. The Patient Consent Subgroup considered the following three options in more detail as methods of addressing this issue:

Patient Consent Issue #3 - Option #3.1: Leave the term “Medical Emergency” undefined.

Advantages of Option #3.1

- This option is consistent with current practice in Minnesota and health care organizations would not need to modify their procedures to accommodate a new, explicit definition of the term “Medical Emergency.”
- The lack of a definition for the term “Medical Emergency” has not created a significant barrier to the exchange of patients’ health information for organizations using paper health records.

Disadvantages of Option #3.1

- This option does not help in resolving differences in those instances where health care providers do not agree if a situation is a medical emergency.
- The lack of a definition for the term “medical emergency,” may make it more difficult to articulate rules that automate the electronic exchange of patients’ health information in medical emergencies.

Other Issues Related to Option #3.1

- As noted in the introduction to this problem, most health care providers believe that current law places all liability for inappropriate disclosure on the disclosing provider. Therefore, variation in assessing a situation as a medical emergency can often be because of a provider's reluctance to rely on a third party's determination that a medical emergency exists.
- This definition does not address a disclosing provider's ability to rely on another provider's determination that a medical emergency exists.
- This option does not address any documentation requirements for the determination of a medical emergency that would provide accountability and a record if the determination is later challenged.

Patient Consent Issue #3 - Option #3.2: Amending Minnesota Statutes, section 144.335, subdivision 1 by adding:

"Medical emergency" means medically necessary care which is immediately necessary to preserve life, prevent serious impairment to bodily functions, organs, or parts, or prevent placing the physical or mental health of the patient in serious jeopardy.

This definition comes from Minnesota Rules 4685.0100, Subpart 5(A), which relates to the regulation of health maintenance organizations.

Advantages of Option #3.2

- This definition is very consistent with the implicit definition that many health care providers use today in determining if a situation is a medical emergency. Therefore, this option would not require significant changes in health care providers' activities.
- A common definition for the term "Medical Emergency" may help to eliminate variation in standards people apply in determining if a situation is a medical emergency, which would help to facilitate and automate the electronic exchange of patients' health information in medical emergencies.
- This definition leaves the physician, or other health care provider, with the responsibility of exercising their judgment and determining whether or not a medical emergency exists.

Disadvantages of Option #3.2

- This definition may not fully resolve variations in health care providers' assessment of situations as emergencies. It is possible that health care providers may not agree on whether or not a situation is a "serious impairment."
- Some Patient Consent Subgroup members questioned whether any definition that allows health care providers to exercise their judgment could result in agreement about whether or not particular instances are medical emergencies. This disadvantage is not a recommendation against definitions that incorporate medical judgment, but rather a recognition that there is always an element of medical judgment in the assessment of situations that may make an absolute definition infeasible.

Other Issues Related to Option #3.2

- As noted in the introduction to this problem, most health care providers believe that current law places all liability for inappropriate disclosure on the disclosing provider.

Therefore, variation in assessing a situation as a medical emergency can often be because of a provider's reluctance to rely on a third party's determination that a medical emergency exists.

- This definition does not address a disclosing provider's ability to rely on another provider's determination that a medical emergency exists.
- This option does not address any documentation requirements for the determination of a medical emergency that would provide accountability and a record if the determination is later challenged.

Patient Consent Issue #3 - Option #3.3: Amending Minnesota Statutes, section 144.335, subdivision 1 by adding:

"Medical emergency" means that immediate medical care is needed to prevent death or a substantial and irreversible impairment of a major bodily function.

This definition is adapted from Indiana Code 16-34-2-1.2.

Advantages of Option #3.3

- This definition provides reasonably clear criteria for determining if a situation is a medical emergency.

Disadvantages of Option #3.3

- This definition is not very consistent with the implicit definition that many health care providers use today in determining if a situation is a medical emergency. Therefore, this option would require significant changes in health care providers' activities.
- The definition would classify fewer situations as medical emergencies than the implicit definition currently used by most health care providers. Making this exception to patient consent more restrictive may negatively impact health care providers' ability to deliver care.
- Some Patient Consent Subgroup members questioned whether any definition that allows health care providers to exercise their judgment could result in agreement about whether or not particular instances are medical emergencies. This disadvantage is not a recommendation against definitions that incorporate medical judgment, but rather a recognition that there is always an element of medical judgment in the assessment of situations that may make an absolute definition infeasible.
- This definition does not address a disclosing providers' ability to rely on another providers' determination that an emergency exists.

Other Issues Related to Option #3.3

- As noted in the introduction to this problem, most health care providers believe that current law places all liability for inappropriate disclosure on the disclosing provider. Therefore, variation in assessing a situation as a medical emergency can often be because of a provider's reluctance to rely on a third party's determination that a medical emergency exists.
- This definition does not address a disclosing provider's ability to rely on another provider's determination that a medical emergency exists.

- This option does not address any documentation requirements for the determination of a medical emergency that would provide accountability and a record if the determination is later challenged.

Patient Consent Issue #4:

The term "Related Health Care Entity" is not defined in Minnesota Statutes § 144.335. Another exception to the patient consent requirements exists when health information needs to be disclosed to a "related health care entity." This exception generally allows multi-provider and multi-site health care organizations to release patients' health information to various providers and facilities within the organization as patients receive care from different providers and locations. While the term is not defined in Minnesota Statutes, most health care providers interpret the term to mean organizations owned, operated or controlled by the same legal entity. However, many providers have suggested other interpretations such as:

- Health care entities that have a contractual relationship are related health care entities; or
- Health care entities that share employees 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. The Patient Consent Subgroup considered the following two options as methods of addressing this issue:

Patient Consent Issue #4 - Option #4.1: Amending Minnesota Statutes, section 144.335, subdivision 1 by adding two definitions:

"Affiliate" has the meaning given in section 144.6521, subdivision 3(b).

"Related health care entity" means an affiliate of the provider releasing the health information.

Advantages of Option #4.1

- This definition is consistent with the implicit definition for the term "Related Health Care Entity" currently used by most health care providers. Therefore, this option would not require significant changes in health care providers' activities.
- This definition is clear, understandable and built on existing Minnesota law.
- This definition helps to ensure patients' privacy protections because it limits the ability to disclose patient information under this exception for patient consent. Under this definition patients' health information can only be released among providers who are commonly controlled.
- By adding clarity to the meaning of the term "Related Health Care Entity," this definition would increase agreement on "when" patient consent is needed to disclose/exchange patients' health information. This clarity would help in two ways. First, it would help to facilitate and automate the electronic exchange of patients' health information. Second, it would help patients to better understand "when" and "how" they can exercise some control over their health information.
- Some Patient Consent Subgroup members believe that the legislative history related to this issue indicates that the Legislature intended this exception to cover situations where there

was some common control over the parties exchanging patients' information. Hence, this definition may be consistent with the original legislative intent.

Disadvantages of Option #4.1

- For health care providers that use a more expansive definition of the term "Related Health Care Entity," this definition would require significant changes in health care providers' activities.

Patient Consent Issue #4 - Option #4.2: Amending Minnesota Statutes, section 144.335, subdivision 1 adding two definitions:

"Affiliate" has the meaning given in section 144.6521, subdivision 3(b).

"Related health care entity" means any person is an affiliate or that has a contractual relationship with a provider.

Advantages of Option #4.2

- This definition is a more expansive definition that would permit patients' health information to be exchanged in more situations without patients' consent. This may be helpful in ensuring that health care providers have the necessary health information to deliver appropriate care to patients.
- This definition is consistent with patients' expectations that an admitting physician, who is not a hospital employee, gets information on the patient's hospitalization. However, there may be other portions of Minnesota's patient consent requirements that accomplish the same purpose.
- This definition could make it easier and less expensive for health care organizations' implementation of Minnesota's patient consent requirements, because this more expansive definition would require organizations to document and track fewer patient consents.

Disadvantages of Option #4.2

- This definition is not consistent with the implicit definition for the term "Related Health Care Entity" currently used by most health care providers. Therefore, this option could require significant changes in health care providers' activities.
- This definition potentially reduces patients' ability to control the disclosure/exchange of their health information, because contractual relationships between providers could be established to avoid obtaining patients' consent to disclose health information.
- Some Patient Consent Subgroup members believe that this definition yields more opportunities for the inappropriate disclosure and possible abuse of patients' health information, because contractual relationships between providers could be established to avoid obtaining patients' consent.
- Some Patient Consent Subgroup members believe that the legislative history related to this issue indicates that the Legislature intended this exception to cover situations where there was some common control over the parties exchanging patients' information. Hence, this definition may not be consistent with the original legislative intent.
- Contractual relationships between providers can be established or dissolved at any time. So while this definition adds clarity to the term "Related Health Care Entity," it may not

help patients understand “when” and “how” they are able to control their health information.

Patient Consent Issue #5:

Long term care providers experience situations where a patient's health information is needed to deliver appropriate care, but it is impossible to obtain the information because the patient is physically or mentally unable to provide consent for the health information to be released to the long term care facility. This issue is linked to Patient Consent Issue #4 because many long term care providers have suggested that the term “Related Health Care Entity” should have a more expansive definition in order to address a specific need of long term care facilities. Specifically, long term care providers often need to transfer residents to a hospital for treatment or emergency care. When it is time for the patient to be released from the hospital and return to the long term care facility, the patient's consent is needed for the hospital to provide the long term care facility with health information necessary for continuing care. However, as many as 40% of long term care facility residents suffer from varying degrees of dementia and are incapable of providing consent for the release of health records. Yet, the long term care facility cannot deliver appropriate care without receiving the patient's health information.

During Patient Consent Subgroup meetings, it was suggested that this issue could be better addressed directly, rather than through the definition of the term “Related Health Care Entity.” The following option reflects the subgroup's discussion of this issue:

Patient Consent Issue #5 - Option #5.1: Amending Minnesota Statutes, section 144.335, subdivision 3a as follows:

(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- ;

(3) to a health care facility licensed by this chapter, chapter 144A, or to the same types of health care facilities licensed by this chapter and chapter 144A that are licensed in another state when a patient:

(i) is returning to the health care facility and who is unable to provide consent; or

(ii) who resides in the health care facility and has services provided by an outside resource under 42 CFR section 483.75(h) and is unable to provide consent.

Advantages of Option #5.1

- o This option addresses the specific difficulties faced by long term care providers in trying to comply with both Minnesota's patient consent requirements and Minnesota's requirements related to delivering appropriate continuity of care. This option will help to ensure that long term care providers are able to obtain patients' health information in order to appropriately deliver care.

- This option addresses cross-border situations by including long term care facilities licensed in other states.
- This option's exception to needing patient consent is limited to situations where the patient is unable to provide consent. Therefore, patients with the physical and mental ability to provide consent retain the ability to exercise control over their information.
- This option is also limited in that it clearly indicates who information may be released to without consent.

Disadvantages of Option #5.1

- The meaning of "unable to provide consent" is open to various interpretations. Specifically, does this phrase mean unable to provide consent in the professional judgment of the provider disclosing the health information? Also, is specific documentation needed to note patients' inability to provide consent?
- This language could be used to avoid obtaining consent from a health care agent under a health care power of attorney.

Patient Consent Issue #6:

There is a need to define and introduce the concept and term "Record Locator Service" in Minnesota Statutes § 144.335. 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. A record locator service functions as an index or card catalog for patient records; the record locator service stores sufficient identifying information to uniquely identify each patient and provides pointers to the locations of patients' health information. The record locator service only contains the identifying information necessary to assist providers in finding the location of all pertinent health information; it does not contain the patients' clinical data.

Because a record locator service does not contain clinical data - other than clinic name - there is disagreement about "how" Minnesota's patient consent requirements apply to the information in a record locator service. To resolve these disagreements and to facilitate electronic exchange of health information, it is necessary to:

1. Define the concept of a record locator service;
2. Determine what identifying information can be included in a record locator service (see also – Patient Consent Issue #2); and
3. Clarify if and how Minnesota's patient consent requirements apply to a record locator service.

The Patient Consent Subgroup considered the following two options as methods of addressing this issue:

Patient Consent Issue #6 - Option #6.1: Amending Minnesota Statutes, section 144.335, subdivision 1 by adding:

"Record locator service" means an electronic index of patient identifying information that directs participants in a health information exchange to the location of patient health records held by providers as defined in section 144.335, subdivision 1(b) and group purchasers as defined in section 62J.06, subdivision 6.

This option also assumes that the term "Identifying Information" has been added to Minnesota Statutes § 144.335, Subdivision 1.

Advantages of Option #6.1

- This definition is flexible enough to encompass a variety of different models for a record locator service, including different data elements to be used as identifying information. This definition is linked to the possible definitions of "Identifying Information" described in Patient Consent Issue #2.
- This definition limits the information that can be included in a record locator service to non-clinical, patient identifying information and the location of the health record. By not including clinical data in the record locator service, this definition helps to protect patients' privacy and limit the possibility of inappropriate disclosures of patient health information.
- This definition of the term limits its use to participants in a Health Information Exchange.
- This definition allows the record locator service to point to health records held by providers, as well as health records held by group purchasers (e.g., health plans). By including both providers and group purchasers this definition would point to a more complete set of health information. It is necessary to include group purchasers to get a complete health record, because health plans have more complete records than health care providers in some areas (e.g., medication history).

Disadvantages of Option #6.1

- Even though this definition does not include clinical data in the record locator service, it is possible that simply identifying the name of the clinic could reveal health information about a patient (e.g., mental health or substance abuse treatment facility).
- This definition is limited to Minnesota providers and group purchasers. This limitation may have a negative effect on patients living near Minnesota's borders because care may be delivered across state lines. If the definition is broadened to include providers in other states, there is no guarantee that the other states have the same privacy protections for information in a record locator service.
- This definition does not clearly include some entities that would have health records that may be useful for providers treating patients. Specifically, there may be other types of health care providers than those defined in Minnesota Statutes § 144.335, Subdivision 1. The definition of provider under HIPAA would include other types of providers not included in this definition. Similarly, some governmental entities, such as the Department of Health, may not be covered by this definition.
- Allowing a record locator service to identify the location of health records held by group purchasers may foster suspicion or concern with patients, because group purchasers hold

patient information beyond that information needed for treatment. However, this disadvantage is reduced by the fact that this definition does not include clinical data in the record locator service.

Patient Consent Issue #6 - Option #6.2: Amending Minnesota Statutes, section 144.335, subdivision 1 by adding:

“Record locator service” means an electronic index of patient identifying information that directs participants in a health information exchange to the location of patient health information held by providers as defined in section 144.335, subdivision 1(b).

This option also assumes that the term “Identifying Information” has been added to Minnesota Statutes § 144.335, Subdivision 1.

Advantages of Option #6.2

- This definition is flexible enough to encompass a variety of different models for a record locator service, including different data elements to be used as identifying information. This definition is linked to the possible definitions of “Identifying Information” described in Patient Consent Issue #2.
- This definition limits the information that can be included in a record locator service to non-clinical, patient identifying information and the location of the health record. By not including clinical data in the record locator service, this definition helps to protect patients’ privacy and limit the possibility of inappropriate disclosures of patient health information.
- This definition of the term limits its use to participants in a Health Information Exchange.
- By not allowing a record locator service to identify the location of health records held by group purchasers, this definition may help to alleviate patients’ suspicion or concern about non-treatment, patient information held by group purchasers.

Disadvantages of Option #6.2

- Even though this definition does not include clinical data in the record locator service, it is possible that simply identifying the name of the clinic could reveal health information about a patient (e.g., mental health or substance abuse treatment facility).
- This definition allows the record locator service to point to health records held by only providers. By limiting this definition to just providers, the record locator service would point to a less complete set of health information. It is necessary to include group purchasers to get a complete health record, because health plans have more complete records than health care providers in some areas (e.g., medication history).
- This definition is limited to Minnesota providers. This limitation may have a negative effect on patients living near Minnesota’s borders because care may be delivered across state lines. If the definition is broadened to include providers in other states, there is no guarantee that the other states have the same privacy protections for information in a record locator service.
- This definition does not clearly include some entities that would have health records that may be useful for providers treating patients. Specifically, there may be other types of

health care providers than those defined in Minnesota Statutes § 144.335, Subdivision 1. The definition of provider under HIPAA would include other types of providers not included in this definition. Similarly, some governmental entities, such as the Department of Health, may not be covered by this definition.

Patient Consent Issue #7:

It is unclear if patient consent is needed to place data (i.e., identifying information and provider name) in a "Record Locator Service." Health care providers have traditionally collected, maintained, and exchanged patients' health records in a paper format, and the concept of a record locator service was never developed. Now that providers are looking to develop electronic, Health Information Exchanges capable of automated, real-time information exchange, there is a need to automate the process of identifying the location of patients' health information through a record locator service. However, because the concept of a record locator service is new to electronic exchange, there is disagreement about how Minnesota's patient consent requirements apply to the implementation of a record locator service. That is, there is no agreement about "when" and "how" patient consent is needed to create and/or use a record locator service. This issue is also important to patients, because it determines "how" they are able to control disclosures of their identifying and health-related information.

The Patient Consent Subgroup considered the following three options as methods of addressing this issue:

Patient Consent Issue #7 - Option #7.1: Amending Minnesota Statutes, section 144.335 with a subdivision that states:

Subd. Q. [Record Locator Service.] A provider [or group purchaser as defined in section 62J.06, subdivision 6] shall obtain consent to send patient identifying information and information about the location of the patient's health records to a record locator service. Consent from a patient to provide identifying information and information about the location of the patient's health records to a record locator service does not expire. The patient may revoke that consent at any time by providing written notice of the revocation to the provider [or group purchaser as defined in section 62J.06, subdivision 6].

This option requires patient consent prior to sending information about the location of patients' health records to a record locator service. This option also assumes that the terms "Record Locator Service" and "Identifying Information" have been added to Minnesota Statutes § 144.335, Subdivision 1.

Advantages of Option #7.1

- This option allows the patient to choose which providers may send information to a record locator service.
- This option would allow patients to know what information is included in the record locator service prior to information being included.
- This option continues to provide patients a measure of control over their information by requiring consent to include information and allowing that consent to be revoked at any time.
- By requiring that patient consent be obtained, this option gives providers an opportunity to inform and educate patients about the benefits of electronically exchanging health information and contributes to a broader understanding of health care reform. It also allows patients to be informed about the record locator service, the benefits of including

information, and the risks of including, or not including, information in the record locator service.

Disadvantages of Option #7.1

- Under this option a Health Information Exchange may not reach its full potential for improved patient treatment, because the record locator service is incomplete about the location of patients' health records. If the patient has not consented to information being sent to the RLS, then the location of the records will not appear and this would impede the ability of a provider to access those health records, particularly to an emergency.
- For patients who do not consent to information being included in a record locator service, important health information needed for treatment may not be able to be exchanged in real time; that is, providers would likely need to manually exchange patients' health records via paper. One of the advantages of electronically exchanging health information is that it can facilitate the availability of needed health information at the time care is being delivered.
- The patient would have to give consent at each provider for information to be sent to the record locator service. Although this allows patients greater control, it places a greater administrative burden on both patients and the providers, because it requires more forms for patients to complete, more pages to read and more time to understand.
- The consent would have to specify who was participating in the Health Information Exchange and using the record locator service. Hence, the patient consent would need to be written and mechanisms developed to handle changes in the organizations participating in the Health Information Exchange to ensure that any changes in the Health Information Exchange participants would not require that new consents be obtained.
- The patient consent process could create an operational burden for providers. Not only would the provider have to obtain the consent, it would have to be stored and records kept so that if a revocation occurs, the provider could take the appropriate action.
- Although requiring that patient consent be obtained gives providers an opportunity to inform and educate patients, it may be difficult for providers to explain a Health Information Exchange and a record locator service in clear, understandable language.
- Under this option, information about the location of patients' health records is less available over the short term. If patients are required to provide consent before information is sent to the record locator service, the information will be filled in slowly over time. This contrasts with having information about the location of patients' health records available if no consent is required.
- Depending on how the patient consent is drafted, there may be problems when two Health Information Exchanges want to coordinate their activities.

Patient Consent Issue #7 - Option #7.2: Amending Minnesota Statutes, section 144.335 with a subdivision that states:

Subd. Q. [Record Locator Service.] A provider [or group purchaser as defined in section 62J.06, subdivision 6] may send patient identifying information and information about the location of the patient's health records to a record locator service without consent from the patient. Except in the case

of a medical emergency, a provider participating in a health information exchange using a record locator service cannot access patient identifying information and information about the location of the patient's health records until the patient has provided consent. The consent does not expire and may be revoked by the patient at any time by providing written notice of the revocation to the provider [or group purchaser as defined in section 62J.06, subdivision 6].

This option allows participants in a Health Information Exchange to construct a record locator service without patient consent, but limits a provider's ability to access information about a patient without obtaining the patient's consent, except in the case of medical emergencies. This option has the ability to include, or not include, information about the location of health records held by group purchasers. This option also assumes that the terms "Record Locator Service," "Medical Emergency" and "Identifying Information" have been added to Minnesota Statutes § 144.335, Subdivision 1.

Advantages of Option #7.2

- This option allows patients to choose which providers may access information about the location of their health records through a record locator service.
- In a medical emergency when the patient is unable to consent, health information about patients can be located because the record locator can be accessed in an emergency without patient consent.
- This option continues to provide patients a measure of control over their information by requiring consent for providers to access information contained in a record locator service and allowing that consent to be revoked at any time.
- Depending on the exact mechanisms used to implement this option within a Health Information Exchange, it may be possible to allow patients to designate that a provider is only able to access a subset of information in the record locator service.
- Under this option, information about the location of patients' health records can be made available through a record locator service immediately. This option permits providers and group purchasers to send information to the record locator service as soon as they become participants in a Health Information Exchange.
- This option continues to provide patients a measure of control over their information by requiring consent for providers to access information included in a record locator service and by allowing that consent to be revoked at any time.
- This option provides an efficient mechanism for providers participating in a Health Information Exchange to create a record locator service, because patient consent does not have to be obtained, tracked or managed to place information in the record locator service. While consent is needed to access the information, that consent does not expire and the operational burden of recordkeeping is reduced.
- There may be fewer problems when two Health Information Exchanges want to coordinate their activities, because this option allows patients to provide consent at the point of care.

Disadvantages of Option #7.2

- Patients' ability to control which providers include information in a record locator service is less than under Option #1. All providers and group purchasers send information to the

record locator service and the patient is not able to differentiate which providers or group purchasers are sending information.

- This option may provide patients less opportunity to know what information is being included in a record locator service, because the information is being sent to the record locator service without the patients' consent.
- For patients who do not consent to allowing providers to access information included in a record locator service, important health information needed for treatment may not be able to be exchanged in real time; that is, providers would likely need to manually exchange patients' health records via paper. One of the advantages of electronically exchanging health information is that it can facilitate the availability of needed health information at the time care is being delivered.
- Some patients may believe that their privacy has been reduced by the creation of a record locator service, which contains information about them. Thus even if a patient does not consent to allowing any providers to access the information, they may be concerned about the existence of the record locator service.
- Although requiring that patient consent be obtained gives providers an opportunity to inform and educate patients, it may be difficult for the provider to explain a Health Information Exchange and a record locator service in clear, understandable language.

Patient Consent Issue #7 - Option #7.3: Amending Minnesota Statutes, section 144.335 with a subdivision that states:

Subd. Q. [Record Locator Service.] A provider [or group purchaser as defined in section 62J.06, subdivision 6] may send patient identifying information and information about the location of the patient's health records to a record locator service without consent from the patient. For treatment purposes, a provider may access patient identifying information and information about the location of the patient's health records in a record locator service without consent from the patient.

Advantages of Option #7.3

- This option is the most efficient manner of creating and using a record locator service, because there is no need to obtain, document, or track patients' consent.
- This option would give providers the most complete information about the location of their patients' records, because all providers and group purchasers participating in a Health Information Exchange would be able to send information to the record locator service.
- This option clearly limits providers' use of the record locator service to treatment purposes, which could help to reduce concerns over the fact that consent is not needed to access the information in the record locator service.
- In a medical emergency when the patient is unable to consent, health information about the patient can be located because the record locator service can be accessed without patient consent.
- There may be fewer problems when two Health Information Exchanges want to coordinate their activities, because patient consent issues do not need to be addressed.

Disadvantages of Option #7.3

- This option does not provide patients control over where their information is held or used.
- This option does not seem consistent with Minnesota's culture of protecting patient health related information. Current Minnesota law requires a patient to consent for the disclosure of health information, yet these privacy protections are set aside when no consent from the patient is needed to send or access information in a record locator service.
- This option may provide patients less opportunity to know what information is being included in a record locator service, because the information in the record locator service is being sent and accessed without patients' consent.
- Because patient consent is not obtained, this option does not help facilitate providers in informing and educating patients about the benefits of electronically exchanging health information.

Patient Consent Issue #8:

The concept of "Current Treatment" in Minnesota Statutes § 144.335, Subdivision 3a (c)(1) is not uniformly interpreted and has a significant impact on "when" and "how" patient consent is needed to release health records. 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 statutes 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. Unfortunately, the statutes do not define or clarify the term "current treatment." Consequently, health care providers have adopted at least two different interpretations for the term with very different implications for when the general consent permits a health care provider to release health records to another provider.

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.

The Patient Consent Subgroup considered the different interpretations to identify the advantages and disadvantages of each interpretation:

Patient Consent Issue #8 – Interpretation #8.1: 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. 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;

Advantages of Interpretation #8.1

- Assuming that most patients will sign the general consent, this interpretation:
 - better facilitates the sharing of health information with any provider that is treating the patient.
 - is operationally easier and less costly to implement. The one-time general consent means that there would be fewer specific patient consents to document and track.
 - is more consistent with states along Minnesota's borders.
- This interpretation minimizes the consequences of differences that arise within the definitions of the terms "Medical Emergency" and "Related Health Care Entity." The exceptions to needing patient consent that use the terms "Medical Emergency and "Related Health Care Entity" would not be needed for patients who have signed the general consent.
- Some Patient Consent Subgroup members believe that this Interpretation recognizes the authenticity or legitimacy of a patient's decision to authorize all releases forward into the future and not be required to sign consents each year.
- This interpretation is consistent with some health care providers' current implementation of Minnesota's patient consent requirements.

Disadvantages of Interpretation #8.1

- This interpretation provides patients less detailed control over "when" and "how" their health information is disclosed.
- Patients may not remember all of the times that they have signed a general consent. This point is reinforced by the fact that patients frequently needed to be reminded when and where they signed a consent as part of treatment, particularly when their health information is disclosed to someone or somehow that they did not anticipate.
- Some Patient Consent Subgroup members believe that this interpretation would invite more restrictive statutory language and the need for more specific consents for the release of health information about sensitive conditions such as mental health conditions and HIV status. Other states have found that having many different statutory consent requirements for various conditions is a barrier to electronic exchange of health information.
- This interpretation is not necessarily operationally easier to implement because it rests on the assumption that most patients will sign the general consent. If patients choose not to sign the consent, then providers will need to obtain specific consents for each disclosure of information. The need to obtain specific consents for each disclosure would be more difficult to implement.

- This interpretation provides the patient with less opportunity for understanding what health information is likely to be disclosed and to who the information is to be disclosed. Because the general consent covers any health information that a provider deems relevant to their current treatment of the patient, it is less likely that the patient know or remember what information may be released.

Other Issues Related to Interpretation #8.1

- The Patient Consent Subgroup had an additional discussion questioning the percentage of people that would sign the general consent. In general, most people currently sign the general consent, although it may be under either Interpretation #1 or Interpretation #2 – depending on the provider. Some Patient Consent Subgroup members believe that fewer people would sign the general consent if they were more empowered through education and better understood their ability to exercise more control over their health information.

Patient Consent Issue #8 – Interpretation #8.2: 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;

Advantages of Interpretation #8.2

- This interpretation provides patients more detailed control over "when" and "how" their health information is disclosed.
- This interpretation provides the patient with a better opportunity of understanding what health information is likely to be disclosed and to who the information is to be disclosed. Because the general consent covers only health information related to the releasing provider's current treatment of the patient, it is more likely that the patient understands what information is related to that current treatment.
- This interpretation would put less pressure on patients to remember all of the times that they have signed the general consent.
- Some Patient Consent Subgroup members believed that this interpretation would mean that additional statutory language for specific consents related to sensitive health conditions is less necessary/likely.
- This interpretation is consistent with some health care providers' current implementation of Minnesota's patient consent requirements.

Disadvantages of Interpretation #8.2

- This interpretation requires organizations to document and track more specific consents to disclose health information, because the general consent has a narrower scope.
- For organizations currently following Interpretation #1, this interpretation would require increased effort and cost to obtain and document patients' consent.

- This interpretation is less consistent with providers' ability to exchange health information in border states.
- Some Patient Consent Subgroup members believe that that the annual renewal of consent devalues the patient's previous consent. However, other Subgroup members believe that the annual renewal of consent provides patients greater control over the disclosure of their health records.
- This interpretation increases the importance of the definitions of the terms "Medical Emergency" and "Related Health Care Entity." The exceptions to needing patient consent that use the terms "Medical Emergency" and "Related Health Care Entity" would be needed more often because the general consent has a narrower scope.

Other Issues Related to Interpretation #8.2

- Some Patient Consent Subgroup members believe that Interpretation #2 may become easier to implement over time as electronic health record systems and data standards advance and support more sophisticated exchanges.
- As the exchange of health information moves from paper media to electronic media, there will be increased ability to track who has accessed patients' health data, when it was accessed and why. These increased tracking abilities may impact patients' feelings about how and when they want to provide consent.

Patient Consent Issue #9:

Minnesota law does not provide a mechanism or framework for a provider to rely on another provider's representation of having obtained patient consent to disclose health records. One mechanism that could help facilitate the automated, real-time electronic exchange of patients' health information while maintaining patient consent would be a mechanism/framework that allows patients to provide consent through the requesting provider at the point of service. That is, the patient consent requirements would allow the disclosing provider to automatically and electronically exchange patients' health information to the requesting/treating provider based on the requesting provider's representation of having obtained the patient's consent.

To address this issue, Minnesota law would need to provide a framework and mechanism to transfer/share responsibilities and liability for patient consent between the disclosing and requesting providers. 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 options should minimally address:

1. When a provider disclosing health records may rely on a requesting provider's representation of having obtained patient consent for the requested health records;
2. 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;
3. The liability of a disclosing provider for having released records based on a requesting provider's misrepresentations of having obtained patient consent; and
4. The liability of a requesting provider for misrepresenting that the provider had obtained patient consent when requesting health records.

The Patient Consent Subgroup considered the following two options as methods of addressing this issue:

Patient Consent Issue #9 - Option #9.1: Leave the liability-related portions of Minnesota's patient consent requirements unchanged. This option would simply leave Minnesota Statutes § 144.335 Subdivision 3a, (e) as:

(e) A person who negligently or intentionally releases a health record in violation of this subdivision, or who forges a signature on a consent form, or who obtains under false pretenses the consent form or health records of another person, or who, without the person's consent, alters a consent form, is liable to the patient for compensatory damages caused by an unauthorized release, plus costs and reasonable attorney's fees.

Advantages of Option #9.1

- o This option maintains the status quo, which some Patient Consent Subgroup members believe places liability on both the requesting and disclosing provider.

Disadvantages of Option #9.1

- o This option does not clearly address a disclosing provider's ability to rely on a requesting provider's representation of having obtained patient consent to release health records.
- o Most health care organizations believe that this option (i.e., existing law) places the liability for inappropriate disclosures on the disclosing provider, and therefore makes it nearly impossible to rely on another provider's representation of having obtained patient consent to disclose health records.
- o Providers who are operating under this language today do not rely on other provider's representation of having obtained patient consent to disclose health records. Hence, it is difficult to see how this option would facilitate the automated, real-time electronic exchange patients' health information.

Patient Consent Issue #9 - Option #9.2: Divide liability among the parties involved based on a balancing test. This option would facilitate electronic exchange of health information by allowing a provider requesting health records to obtain the necessary consent from the patient and communicate the fact of the consent to the disclosing provider. This also allows the disclosing provider to rely on the representation of the requester that consent had been obtained from the patient. This option has two parts which all work together.

Amend Minnesota Statutes, section 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

(i) a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release, ;

~~(ii) unless the release is specifically authorized by specific authorization in law; or~~

(iii) a representation from a provider that they hold a consent from the patient.

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.

Add to Minnesota Statutes, section 144.335:

Subdivision 3e. In adjudicating a dispute involving the disclosure of patient health records, a court will use the following in determining how liability will be allocated.

(a) When requesting health records using consent, a person warrants that the consent:

(i) contains no information known to the person to be false; and

(ii) accurately states the patient's desire to have health records disclosed or that there is specific authorization in law.

(b) When requesting health records using consent or the representation authorized in subdivision 3a(a)(iii), a provider warrants that the request:

(i) contains no information known to the provider to be false;

(ii) accurately states the patient's desire to have health records disclosed or that there is specific authorization in law; and

(iii) does not exceed any limits imposed by the patient in the consent.

(c) When disclosing health records, a person warrants that they:

(i) have complied with the requirements of this section regarding disclosure of health records;

(ii) know of no information related to the request that is false; and

(iii) have complied with the limits set by the patient in the consent or as described in the representation of consent.

(d) A court of this state presumes that:

(i) A request made by a person that complies with the provisions of this subdivision is valid and represents the wishes of the patient.

(ii) The information listed in a consent or representation of consent is accurate.

(iii) The recipient of a consent or representation of consent has no knowledge or notice that the person making the request:

(A) breached a duty to the patient; or

(B) does not rightfully have a consent.

(iv) The signature on the consent or representation of consent is not forged.

(v) The consent or representation of consent was not obtained under false pretenses.

(vi) The consent or representation of consent was not altered without the patient's permission.

(e) No person or provider may disclaim or contractually limit the application of this subdivision, nor obtain indemnity for its effects, if the disclaimer, limitation, or indemnity restricts liability for misrepresentation as against persons reasonably relying on the consent, representation of consent, or disclosure.

(f) A court of this state shall give effect to liability allocations between the parties provided by contract that do not allocate liability to the detriment of the patient and to the extent the allocation is consistent with the requirements of this chapter.

(g) A patient is eligible to receive compensatory damages plus costs and reasonable attorney's fees if the provisions of this section are violated.

Advantages of Option #9.2:

- This option provides a framework and mechanism to transfer/share responsibilities and liability for patient consent between the disclosing and requesting providers.
- This option maintains all of the patient protections against inappropriate disclosures that currently exist in Minnesota Statutes § 144.335, Subdivision 3a (e).
- This option facilitates patients' ability to consent to a provider accessing their health records at the point of care, which has a number of advantages:
 - it provides patients with the opportunity to make the decision at the present time, as distinct from some time in the past when they may or may not have anticipated future health care needs
 - it provides patients the opportunity to easily take advantage of the current provider's expertise and judgment about what health care records are relevant to the patient's current health care problems or needs
 - in connection with a record locator service, it enables the current provider and the patient to escape the limitations of the patient's memory about providers previously consulted.
 - it ensures that a larger set of health records are available to the treating provider.
- This option only permits health care providers to request the release of health records based on their representation. This minimizes the opportunity for inappropriate disclosures for non-treatment purposes.
- Technology could be used in a Health Information Exchange to capture the data needed to document providers' representations that patient consent was given. Within a Health Information Exchange, the ability to document providers' representations facilitates the ability to verify compliance.
- The language in subdivision 3e(b)(ii) would be an incentive for providers in an electronic environment to quickly and accurately record revocations and other statements of limitation so that the system could identify potential problems with the disclosure of patients' health information.

- This option would be conducive to the development of a standard patient consent form that would offer all participants a “safe harbor” to assist in managing the risk of inappropriate disclosures.

Disadvantages of Option #9.2:

- Patients’ ability to limit the disclosure of health records to treating providers can have a negative impact on the care that the patient receives. Incomplete disclosure also may expose health providers to malpractice claims. However, these facts are also true today. This disadvantage highlights that a patient may suffer consequences for choosing not to consent to the release of health records. However, this concern could be addressed by a statement in the consent that partial release of records will affect patient care.
- This amendment that acknowledges the ability to rely on a representation of having consent is limited to health care providers.
- By maintaining existing language stating that consents must be written and signed, the oral communication that does occur among providers is not addressed. Participants were unsure whether this practice of sharing information about patients by providers could be completely eliminated.

Other Issues Related to Option #9.2:

- There was some discussion about the need for a public conversation about consent, what it means and how patients achieve choice in the process. More clarity on the consent form is one option as is education to help patients understand that they don’t have to sign the consent in order to see the provider.
- Currently, some patients use the ability to limit the disclosure of health records for “inappropriate” purposes. For example, patients who are seeking drugs will not authorize complete disclosures to assist them in obtaining drugs. Others ask that their records be changed to show a longer history of a particular condition to make them eligible for some kinds of care (e.g. through the Veteran’s Administration). There was concern that enabling electronic exchange of health information will exacerbate this situation.
- On a related note, it was recognized that there is no current statutory authority for providers or health plans to provide information to the appropriate authorities about certain behaviors like those of drug-seekers.

INFORMED CONSENT AND ENFORCEMENT

The Patient Consent Subgroup discussed a number of issues related to the definition of the concept and term “Informed Consent.” Although staff was unable to summarize the discussion for inclusion in this Interim Report, the discussion will be included in the final report.

Similarly, the Patient Consent Subgroup discussed potential modifications to the enforcement mechanisms associated with Minnesota’s patient consent requirements. Those discussions will also be added to the final report.

OVERVIEW OF AUTHORIZATION, AUTHENTICATION, ACCESS CONTROL, AND AUDITING ISSUES

The second overarching privacy and security issue that must be solved to advance the automated, real-time electronic exchange of health information is the development of a framework for addressing four interrelated 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 the patient data that is appropriate for the individual's functions and needs; and
- Mechanisms for coordinated auditing across organizations to identify authorized individuals who inappropriately access health information.

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 and 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.

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.

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 and behavioral controls. 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.

The fourth issue facing organizations in a Health Information Exchange is the need to develop mechanisms for coordinated auditing of individuals' access to health information across organizations. Auditing individuals' access to patients' health information is critical to protecting the privacy and confidentiality of health information. 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 other organizations within the Health Information Exchange to share 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.

GENERAL PRINCIPLES FOR AUTHORIZING AND AUTHENTICATING INDIVIDUALS, SETTING ACCESS CONTROLS, AND AUDITING IN A HEALTH INFORMATION EXCHANGE

Specific solutions to the issues identified as authorization, authentication, access control, and auditing issues will depend on a number of factors beyond the control of this project. For example, the architecture of a Health Information Exchange, the information technologies used by health care organizations, the standards currently being developed in national efforts, and health care organizations' experience in exchanging information will all significantly influence the framework and mechanisms used to address these issues.

To provide Minnesota health care organizations a foundation and framework for the continued development of Health Information Exchanges, the 4A Subgroup identified a number of general principles that can guide organizations' decision making in forming and implementing Health Information Exchanges. The general principles form a "conceptual solution" that was developed to be:

- independent of a Health Information Exchange's architecture;
- flexible enough to adapt to changes in information technology;
- consistent with national standards currently under development; and
- capable of being refined and more finely detailed as health care organizations gain experience in implementing the electronic exchange of health information

The 4A Subgroup made five general assumptions regarding Health Information Exchanges as part of their discussion and analysis of these issues. The Subgroup also identified nineteen general principles that health care organizations and Health Information Exchanges should address as part of implementing an exchange. In addition to identifying the general principles, the Subgroup provided:

- discussion, analysis, and rationale for each principle;
- recommended resources that may be useful for the further refinement and development of the principles to address changes and/or greater clarity in the architecture of a Health Information Exchanges, information technologies, standards under development, and health care organizations' experience; and
- recommended expertise needed for the further refinement and development of the principles to address changes and/or greater clarity in the architecture of a Health Information Exchanges, information technologies, standards under development, and health care organizations' experience.

The report first presents all of the assumptions and principles without discussion and then presents an expand discussion and analysis of each of the principles:

Assumptions

- A.1** A Health Information Exchange will require all participants to sign a standard participation agreement. This agreement will specify the terms of the relationship and the roles, rights and responsibilities of each party. The signing of this agreement means that each participant will adhere to the policies and procedures of the Health Information Exchange.

- A.2** Health Information Exchanges will define the type of patient health information to be exchanged or accessed between organizations participating in a Health Information Exchange.
- A.3** Health Information Exchanges will exchange patients' health information using national standards for data content and data definitions.
- A.4** The exchange of patient health information through a Health Information Exchange will occur using standard-based messaging and/or view-only access to provider's electronic health records.
- A.5** All organizations participating in a Health Information Exchange will have adopted and implemented generally accepted security programs, policies, and procedures to ensure the confidentiality, integrity, and availability of patients' health information.

Authorization Principles

- P1.1** All individuals having access to patients' health information through a Health Information Exchange will be assigned a unique ID for accessing the health information. Consistent with the authentication principles, each ID for accessing patients' health information shall require at least single-factor authentication (e.g., password) to access health information.
- P1.2** When an individual is granted access to patients' health information through a Health Information Exchange from a particular organization participating in a Health Information Exchange, it should be that participating organization's responsibility to authorize, maintain, and terminate the individual's access to patient health information.
- P1.3** The ability of individuals to access patients' health information through a Health Information Exchange should be set using role-based access standards which are developed and accepted by all organizations participating in a Health Information Exchange.
- P1.4** All organizations participating in a Health Information Exchange should develop and accept security credentialing guidelines for authorizing individuals to access patients' health information through a Health Information Exchange. The security credentialing guidelines and process should be as streamlined as possible and minimally include: a) verifying the identity of individuals authorized to access/exchange health information; b) defining the appropriate role-based access for individuals authorized to access/exchange health information; and c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.
- P1.5** Medical credentialing of health care providers (distinct from security credentialing) should not be required by organizations participating in a Health Information Exchange when the health care provider is only exchanging health information using standard-based messages or accessing health information in view-only access.

Authentication Principles

- P2.1** All organizations participating in a Health Information Exchange should minimally require single-factor authentication for verifying the identity of all individuals authorized to access patients' health information within each organization.
- P2.2** All organizations participating in a Health Information Exchange should minimally require two-factor authentication for verifying the identity of all individuals accessing patients' health information through the Health Information Exchange (i.e., across participating organizations).

P2.3 Authentication of individuals accessing patients' health information through a Health Information Exchange should be as seamless as possible when accessing information across participating organizations.

P2.4 From the end-user's perspective (i.e., health care providers), the authentication of individuals accessing patients' health information through a Health Information Exchange should be the same process regardless of which participating organization's health information is being accessed.

Access Control Principles

P3.1 Health care providers should only access information for patients with whom they have a treatment relationship and then only the health information relevant to the treatment being provided.

P3.2 All organizations participating in a Health Information Exchange should develop and accept written policies and procedures for accessing and exchanging patients' health information through the Health Information Exchange.

P3.3 All organizations participating in a Health Information Exchange should develop and accept minimum standard training requirements for educating individuals about the policies and procedures for accessing/exchanging patients' health information through a Health Information Exchange.

P3.4 All organizations participating in a Health Information Exchange should develop and accept common sanction policies for addressing situations when individuals violate the policies and procedures for accessing/exchanging patients' health information through the Health Information Exchange.

P3.5 Health Information Exchanges should develop policies and procedures for disabling individuals' access to patients' health information through a Health Information Exchange for inappropriately accessing patients' health information.

P3.6 Health Information Exchanges should have policies and procedures for terminating a logged-in individual's session accessing patients' health information due to inactivity within the session.

Auditing Principles

P4.1 All organizations participating in a Health Information Exchange should develop and accept minimum standards for routine auditing of individuals' access to patients' health information through the Health Information Exchange.

P4.2 All organizations participating in a Health Information Exchange should maintain audit logs that document individuals accessing patients' health information. The audit logs should minimally identify: a) the individual accessing the health information; b) the health information being accessed; c) the date and time of the access; and d) all failed log-ins.

P4.3 All organizations participating in a Health Information Exchange should develop and accept: a) the data elements to be maintained and exchanged for auditing individuals' access to patient health information; b) the frequency at which the auditing data will be exchanged between organizations participating in the Health Information Exchange; and c) the minimum retention time of audit logs maintained for auditing individuals' access to patient health information.

P4.4 All organizations participating in a Health Information Exchange should develop and accept procedures for: a) alerting other participating organizations of situations where patients' health

information may have been inappropriately accessed; and b) jointly investigating situations where patients' health information may have been inappropriately accessed.

EXPANDED DISCUSSION AND ANALYSIS OF GENERAL PRINCIPLES

The 4A Subgroup's discussion and analysis of the general principles for authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange was done assuming that the following assumptions are true:

- A.1** A Health Information Exchange will require all participants to sign a standard participation agreement. This agreement will specify the terms of the relationship and the roles, rights and responsibilities of each party. The signing of this agreement means that each participant will adhere to the policies and procedures of the Health Information Exchange.
- A.2** Health Information Exchanges will define the type of patient health information to be exchanged or accessed between organizations participating in a Health Information Exchange.
- A.3** Health Information Exchanges will exchange patients' health information using national standards for data content and data definitions.
- A.4** The exchange of patient health information through a Health Information Exchange will occur using standard-based messaging and/or view-only access to provider's electronic health records.
- A.5** All organizations participating in a Health Information Exchange will have adopted and implemented generally accepted security programs, policies, and procedures to ensure the confidentiality, integrity, and availability of patients' health information.

Authorization Principle P1.1:

All individuals having access to patients' health information through a Health Information Exchange will be assigned a unique ID for accessing the health information. Consistent with the authentication principles, each ID for accessing patients' health information shall require at least single-factor authentication (e.g., password) to access health information.

Discussion and Analysis:

This principle is an adaptation of the HIPAA Security regulation requirement that all individuals granted access to electronic protected health information be assigned a unique name and/or number for identifying and tracking users' identity (45 CFR 164.312(a)(2)(i)). This principle also incorporates the HIPAA Security regulation requirement that organizations implement procedures to authenticate/verify that an individual seeking access to electronic protected health information is who they claim (45 CFR 164.312(d)). This principle allows organizations and Health Information Exchanges to create audit logs that monitor and track individuals' access and use of patients' health information.

The 4A Subgroup also recommends that the unique ID not have any other required characteristics beyond being unique across organizations. For example, the unique ID should not contain embedded intelligence, such as user or organization name or location.

The 4A Subgroup believes that this principle represents the standard practice within health care organizations and does not need additional development

Authorization Principle P1.2:

When an individual is granted access to patients' health information through a Health Information Exchange from a particular organization participating in a Health Information Exchange, it should be that participating organization's responsibility to authorize, maintain, and terminate the individual's access to patient health information.

Discussion and Analysis:

This principle assigns organizational responsibility for all individuals that access patients' health information through a Health Information Exchange. An individual is granted access to patients' health information because at least one organization participating in the Health Information Exchange has determined that the individual needs the access for their job functions.

This principle identifies three required activities for organizations that grant individuals access to patient health information through a Health Information Exchange:

- Authorize the individual – The organization should conduct those activities needed to authorize the individual, such as verifying identity, setting role-based access, and providing authentication information and tools.
- Maintain appropriate access – The organization should maintain individuals' access consistent with their roles and job functions. Hence, if an individual changes roles or job functions, it is the responsibility of the authorizing organization to ensure that those changes are communicated to the Health Information Exchange. This means that organizations may need to perform periodic reviews of individuals' access to the Health Information Exchange to properly maintain individuals' access to health information.
- Terminate access – When it is no longer appropriate for an individual to have access to patients' health information the authorizing organization should terminate that access to the Health Information Exchange.

A health care provider working at multiple organizations participating in a Health Information Exchange may be authorized by more than one organization. However, at least one of the organizations must take responsibility for ensuring appropriate access.

Recommended Resources for Further Development:

- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"
- The policies and procedures of other Health Information Exchanges.

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in the development of the policies and procedures used to implement this principle:

- IT security professionals
- Health information managers
- Human resources
- Legal counsel

Authorization Principle P1.3:

The ability of individuals to access patients' health information through a Health Information Exchange should be set using role-based access standards which are developed and accepted by all organizations participating in a Health Information Exchange.

Discussion and Analysis:

This principle is based on the HIPAA Privacy regulations minimum necessary principle that requires organizations to make reasonable efforts to limit access/disclosures of protected health information to the minimum necessary for accomplishing the intended purpose of the use or disclosure. Most health care organizations currently use some type of role-based access to limit individuals' access to patients' health information. Unfortunately, organizations define their roles differently, so there is a need to create a common framework for role-based access when exchanging information through a Health Information Exchange.

This principle does not require that all organizations use the same framework for role-based access within their organizations. Rather, the principle recommends developing an agreed upon set of roles for exchanging information between organizations through the Health Information Exchange.

Recommended Resources for Further Development:

Health Information Exchanges that develop role-based access standards may find the following national efforts useful in implementing a standard that is likely to be consistent with other Health Information Exchanges:

- ISO/CD TS 21298, "*Health informatics -- Functional and structural roles*"
- ASTM E1986, "*Standard Guide for Information Access Privileges to Health Information*"
- Best practices and recommendations from professional organizations such as:
 - American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)
 - Health Information Management Systems Society (HIMSS)

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in the development of the policies and procedures used to implement this principle:

- Health care providers and others that need access to patients' health information to accomplish their job functions
- Health information managers
- IT security and operations professionals
- Human resources

Authorization Principle P1.4:

All organizations participating in a Health Information Exchange should develop and accept security credentialing guidelines for authorizing individuals to access patients' health information through a Health Information Exchange. The security credentialing guidelines

and process should be as streamlined as possible and minimally include: a) verifying the identity of individuals authorized to access/exchange health information; b) defining the appropriate role-based access for individuals authorized to access/exchange health information; and c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.

Discussion and Analysis:

This principle identifies the minimum set of activities an organization needs to perform when authorizing an individual to access information through a Health Information Exchange. The requirements of this principle are based on, and consistent with, other principles. For example, this principle recommends that an individual be granted an appropriate level of access to patients' health information through a Health Information Exchange based on the role-based access standards developed in Principle 1.3.

This principle uses the term "security credentialing" to denote the activities needed to grant individuals access to health information through a Health Information Exchange. The term was used to distinguish those activities from other credentialing that might be performed by health care organizations, such as medically credentialing a provider to practice medicine in a facility. The 4A Subgroup believes the security credentialing process needs to be as streamlined as possible. That is, the process should require those procedures and activities necessary to ensure that individuals' access is appropriate and secure, but should not contain other procedures not directly related to granting access to the Health Information Exchange.

Recommended Resources for Further Development:

Health Information Exchanges may find the following state and national efforts useful in developing policies and procedures for security credentialing:

- The experiences of other Health Information Exchanges, such as the Community Health Information Collaborative (CHIC).
- ISO/CD TS 21298, "*Health informatics -- Functional and structural roles*"
- ISO/TS 21091:2005, "*Health informatics -- Directory services for security, communications and identification of professionals and patients*"

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in the development of the policies and procedures used to implement this principle:

- IT security and operations professionals
- Health information managers
- Human resources

Authorization Principle P1.5:

Medical credentialing of health care providers (distinct from security credentialing) should not be required by organizations participating in a Health Information Exchange when the health care provider is only exchanging health information using standard-based messages or accessing health information in view-only access.

Discussion and Analysis:

This principle recommends maintaining the same level of medical credentialing requirements for exchanging patients' health information electronically that are currently used for paper records.

Medical credentialing are those activities needed to verify that a provider is appropriately qualified to practice medicine in a health care organization and includes activities such as verifying licensure and certifications. Medical credentialing is an expensive and time-consuming process. Currently, health care organizations exchange patients' health information without requiring that the requesting provider be medically credentialed by the disclosing provider. This principle recommends that simply accessing patients' health information, without the ability to change the record, should not require medical credentialing.

Some organizations' medical credentialing process is linked to their security credentialing process. That is, a provider who needs to be medically credentialed cannot be granted access to electronic health records prior to completing the medical credentialing process. Therefore, organizations may need to modify their processes to implement this principle. Some 4A Subgroup members believe that medical credentialing should be required if a provider has electronic access to all of an organization's electronic patient records. However, it is unclear how this level of credentialing yields greater security for the patients' health records than the security credentialing required in Principle 1.4.

Recommended Resources for Further Development:

Health Information Exchanges may find the following efforts useful in clarifying the requirements for medical credentialing:

- The medical credentialing requirements used by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO)
- The medical credentialing requirements for providers as part of their Medicare participation
- Integrating the Healthcare Enterprise's (IHE) work in developing a common framework to deliver the basic interoperability needed for local and regional health information networks. The work includes a security framework for protecting the confidentiality, authenticity and integrity of patient care data.

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- Medical credentialing staff familiar with JCAHO and Medicare requirements
- IT security and operations professionals
- Health information managers
- Human resources

Authentication Principle P2.1:

All organizations participating in a Health Information Exchange must minimally require single-factor authentication for verifying the identity of all individuals authorized to access patients' health information within each organization.

Discussion and Analysis:

This principle is a corollary to Principle P1.1 and is an adaptation of the HIPAA Security regulations requirement that organizations implement procedures to authenticate/verify that an individual seeking access to electronic protected health information is who they claim to be (45 CFR 164.312(d)).

The 4A Subgroup did not want to be more specific about the type of authentication that may be required and believed that any of the following three possible types of factors could be appropriate:

- o Something the individual knows, such as an ID and password or PIN.
- o Something the individual has, such as, a security fob, smart card or other physical object that must be presented to enable access.
- o Something the individual is, such as, a unique personal biometric (e.g., fingerprint or retina scan).

The 4A Subgroup believes that this principle represents the standard practice within health care organizations and does not need additional development

Authentication Principle P2.2:

All organizations participating in a Health Information Exchange should minimally require two-factor authentication for verifying the identity of all individuals accessing patients' health information through the Health Information Exchange (i.e., across participating organizations).

Discussion and Analysis:

This principle recognizes health care organizations' interests in maintaining a heightened level of security when patients' health information is transmitted, accessed, or exchanged through external networks and connections. This principle is consistent with most health care organizations' current policies related to remote access of electronic health records, which generally require two-factor authentication. As indicated in Principle 2.1 there are many possible authentication mechanisms that could be used to implement this principle. The 4A Subgroup did not want to be more specific about the two authentication factors to ensure that organizations and Health Information Exchanges have flexibility in implementing this principle.

Recommended Resources for Further Development:

Health Information Exchanges may find the following national efforts useful to help assure consistency with other Health Information Exchanges as they implement this principle:

- o The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic exchange of health information.
- o The eHealth Initiative's and Foundation's workgroups. The eHealth Initiative and the Foundation for eHealth Initiative are independent, non-profit affiliated organizations whose missions are to drive improvement in the quality, safety, and efficiency of healthcare through information and information technology.
- o The Healthcare Information and Management Systems Society (HIMSS) and the General Services Administration (GSA) and their collaboration on a pilot project to demonstrate the use of the Electronic Authentication Service Component in a healthcare setting.

- Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations professionals
- Health information managers
- Health care providers and others that need to access patients' health information to accomplish their job functions

Authentication Principle P2.3:

Authentication of individuals accessing patients' health information through a Health Information Exchange should be as seamless as possible when accessing information across participating organizations.

Discussion and Analysis:

This principle addresses the need to make the process of accessing patients' health information through a Health Information Exchange as easy as possible to facilitate its use by providers. There is empirical evidence that providers are disinclined to search for and access patients' health information as the process for doing so becomes more cumbersome. Therefore, organizations and Health Information Exchanges should try to identify provider authentication mechanisms and processes that fit into providers' work flow to maximize the potential of a Health Information Exchange to improve patient care.

Recommended Resources for Further Development:

Health Information Exchanges may find the following national efforts useful to help assure consistency with other Health Information Exchanges as they implement this principle:

- The experiences of other Health Information Exchanges, such as the Community Health Information Collaborative (CHIC).
- Integrating the Healthcare Enterprise (IHE) and their IT Infrastructure Technical Framework
- The Liberty Alliance Project and their work on federated identity, which seeks to enable a networked world based on open standards where consumers, citizens, businesses and governments can more easily conduct online transactions while protecting the privacy and security of identity information.
- ISO/TS 21091:2005, "*Health informatics -- Directory services for security, communications and identification of professionals and patients*"
- The Healthcare Information and Management Systems Society (HIMSS) and the General Services Administration (GSA) and their collaboration on a pilot project to demonstrate the use of the Electronic Authentication Service Component in a healthcare setting.

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- Health care providers and others that need to access patients' health information to accomplish their job functions
- IT security and operations professionals
- Health information managers

Authentication Principle P2.4:

From the end-user's perspective (i.e., health care providers), the authentication of individuals accessing patients' health information through a Health Information Exchange should be the same process regardless of which participating organization's health information is being accessed.

Discussion and Analysis:

This principle extends Principle 2.3 by stating that the authentication process should look and act the same to the health care provider regardless of which participating organization's health information is being accessed. By using the same authentication process to access health information from all participating organizations it will be easier for providers to learn and remember the process. Thus, providers will be more likely to search for and access patients' health information from other sources.

The 4A Subgroup does not intend this principle to imply that the technical authentication processes used by organizations to authenticate each others' providers must be the same. The Subgroup recognized that the exact authentication mechanisms might depend on a number of technological issues. However, it is important to address those issues in a manner that causes the least amount of variation in health care providers' activities.

The Subgroup also noted that there may be a need to develop special authentication procedures for access to sensitive health information, such as mental health or substance abuse treatment. Even in these cases, the 4A Subgroup believes that it is important to minimize the variation in the activities required for a provider to access patients' health information.

Recommended Resources for Further Development:

Health Information Exchanges may find the following national efforts useful to help assure consistency with other Health Information Exchanges as they implement this principle:

- The Healthcare Information and Management Systems Society (HIMSS) and the General Services Administration (GSA) and their collaboration on a pilot project to demonstrate the use of the Electronic Authentication Service Component in a healthcare setting.
- ISO/TS 21091:2005, *"Health informatics -- Directory services for security, communications and identification of professionals and patients"*
- Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.
- ASTM E1762-95(2003), *"Standard Guide for Electronic Authentication of Health Care Information"*

Recommended Experts for Further Development:



Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- Health care providers and others that need to access patients' health information to accomplish their job functions
- IT security and operations professionals
- Health information managers
- Electronic health record vendors

Access Control Principle P3.1:

Health care providers should only access information for patients with whom they have a treatment relationship and then only the health information relevant to the treatment being provided.

Discussion and Analysis:

This principle represents an idealized notion of when and how patients' health information should be accessed by health care providers. It is an idealized notion because it is impossible to know a priori what information may be relevant to the treatment of a patient. It is only after a patient has been diagnosed and treated that it is possible to know what health information was relevant to the treatment provided.

There are two types of access controls: 1) behavioral controls set by organizational policies; and 2) enforced information systems' controls. This principle is intended to serve as a behavioral control and guideline for health care providers' in deciding when and how they should access patients' health information. As with other behavior controls, this principle will only be achieved if there are clear policies, provider education, and sanctions developed to support the principle.

There are two reasons it would be impossible to implement this principle as an enforced information system control. First, health care providers have a constantly evolving and complex set of relationships with patients (e.g., treating relationship, consulting relationship with the treating provider etc.). It is not feasible or practical to try to maintain such a list of relationships. Second, it is impossible to know a priori what information may be relevant to the treatment of a patient, and too stringently limiting health care providers' access to patients' health information can have a negative impact on patient care. Therefore, this principle is intended ensure that providers uphold their professional responsibility to self-limit their access to patients' health information to the information needed to provide appropriate patient care.

To ensure that this principle does not inappropriately restrict a provider's access to necessary patient information, the 4A Subgroup believes that it is important to have a broad and inclusive definition of the term "Treatment Relationship." The Subgroup used the following adaptation of the HIPAA definition of treatment in its discussions: "Treatment Relationship" means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Recommended Resources for Further Development:

Health care organizations may find the following national efforts useful in implementing this principle:

- ISO 26000, "*Guidance on social responsibility*"

- ASTM E1869-04, "Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records"
- ASTM E1988-98, "Standard Guide for Training of Persons who have Access to Health Information"
- ASTM E1986-98(2005), "Standard Guide for Information Access Privileges to Health Information"
- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic exchange of health information.
- Best practices and recommendations from professional organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- Health care providers and others that need access to patients' health information to accomplish their job functions
- Training and development staff
- Chief Privacy Officer
- Corporate compliance staff
- Health information managers

Access Control Principle P3.2:

All organizations participating in a Health Information Exchange should develop and accept written policies and procedures for accessing and exchanging patients' health information through the Health Information Exchange.

Discussion and Analysis:

This principle addresses the need and importance of having explicit, written policies and procedures for accessing patients' health information through a Health Information Exchange. As part of their HIPAA compliance activities, most health care organizations have developed and implemented written policies and procedures for electronically accessing health information within their organizations. This principle extends those policies and procedures to health information accessed through a Health Information Exchange.

There are variations in health care organizations' policies and procedures for electronically accessing health information because of differences in organizations' implementation of health technology. It could be very difficult for all organizations participating in a Health Information Exchange to adopt the same internal health information access policy. However, this principle envisions a common policy for accessing health information across organizations. The requirement for written policies and procedures is intended to ensure that there is a reference document that outlines the standards for accessing

health information through a Health Information Exchange. This reference document of written policies and procedures will also be helpful in implementing Principle 3.3 Training and Principle 3.4 Sanctions.

Recommended Resources for Further Development:

Health Information Exchanges may find the following national efforts useful in implementing this principle:

- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"
- ASTM E1986-98(2005), "*Standard Guide for Information Access Privileges to Health Information*"
- ASTM E1869-04, "*Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records*"
- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic exchange of health information.
- The eHealth Initiative's and Foundation workgroups. The eHealth Initiative and the Foundation for eHealth Initiative are independent, non-profit affiliated organizations whose missions are to drive improvement in the quality, safety, and efficiency of healthcare through information and information technology.
- Best practices and recommendations from professional organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- Health information managers
- Legal counsel
- Human resources
- Chief Privacy Officers
- Corporate compliance staff

Access Control Principle P3.3:

All organizations participating in a Health Information Exchange should develop and accept minimum standard training requirements for educating individuals about the policies and procedures for accessing/exchanging patients' health information through a Health Information Exchange.

Discussion and Analysis:

This principle highlights the importance of training and educating individuals about the policies and procedures for accessing patients' health information through a Health Information Exchange. Under Principle 3.2 the organizations participating in a Health Information Exchange will develop a written set of policies and procedures for exchanging patients' information through the exchange. This policy is intended to ensure that all individuals accessing patients' information through the Health information Exchange understand:

- The policies and procedures developed in Principle 3.2
- Their roles and responsibilities in implementing the policies and procedures
- When and how to access patients' health information through the Health Information Exchange under the access policies.

As noted in Principle 3.1, many of the access controls designed to protect patients' health information will be behavioral controls that require providers, and others, to take actions to access information appropriately. However, these behavioral controls will only be effective if:

- The health information access policies and procedures developed under Principle 3.2 are clear; and
- Individuals understand the policies and procedures and their responsibilities within the procedures.

Training individuals to properly access patients' information will be critical to protecting the privacy of patients' health information. Therefore, all organizations participating in a Health Information Exchange will want to ensure that anyone accessing their data has had the necessary training. Depending on the organization and architecture of a Health Information Exchange, it is possible that the Health Information Exchange could conduct the training or audit that individuals have received training.

The 4A Subgroup also noted that this principle is consistent with, and expands on, their organizations' implementation of the "Security Awareness and Training" requirements under the HIPAA Security regulations (see 45 CFR 164.308 (a)(5)(i)).

Recommended Resources for Further Development:

Health care organizations and Health Information Exchanges may find the following national efforts useful in implementing this principle:

- ASTM E1988-98, "*Standard Guide for Training of Persons who have Access to Health Information*"
- ASTM E1869-04, "*Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records*"
- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic exchange of health information.
- Best practices and recommendations from professional organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA).

- Guidance from the Centers for Medicare and Medicaid Services on the implementation of the HIPAA Security regulations, such as the publication, "*HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information.*"

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- Training and development staff
- Health information managers
- Human resources
- Corporate compliance staff

Access Control Principle P3.4:

All organizations participating in a Health Information Exchange should develop and accept common sanction policies for addressing situations when individuals violate the policies and procedures for accessing/exchanging patients' health information through the Health Information Exchange.

Discussion and Analysis:

This principle addresses situations where individuals violate organizations' policies and procedures for accessing patients' health information through a Health Information Exchange. This principle has at least two components that will facilitate the electronic exchange of health information. First, many of the access controls that a Health Information Exchanges utilizes will be behavioral controls. Under this principle, health care organizations and patients will have greater confidence in the effectiveness of those controls when there are consequences for violating the controls. Second, a common sanction policy across all organizations participating in a Health Information Exchange will encourage a more uniform and equitable enforcement of the policies and procedures developed under Principle 3.2.

This principle does not require all organizations participating in a Health Information Exchange to have the same sanction policies for individuals accessing information within each of the organizations. Rather, the principle is intended to ensure that there is a common sanction policy for individuals accessing patients' health information across organizations through the Health Information Exchange.

Recommended Resources for Further Development:

Health care organizations and Health Information Exchanges may find the following national efforts useful in implementing this principle:

- Best practices and recommendations from professional organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)
- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic exchange of health information.

- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"
- Guidance from the Centers for Medicare and Medicaid Services on the implementation of the HIPAA Security regulations, such as the publication, "*HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information.*"

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- Legal counsel
- Human resources
- Corporate compliance staff
- Health information managers
- Union representatives

Access Control Principle P3.5:

Health Information Exchanges should develop policies and procedures for disabling individuals' access to patients' health information through a Health Information Exchange for inappropriately accessing patients' health information.

Discussion and Analysis:

This principle identifies one mechanism that Health Information Exchanges can use to protect patients' health information from being inappropriately accessed through a Health Information Exchange. Under Principles 3.1 and 3.2 organizations participating in a Health Information Exchange will have developed policies and procedures that define appropriate access to patients' information. This principle for Health Information Exchanges is similar to the HIPAA Security regulations requirement that health care organizations implement procedures for terminating individuals access to patients' health information (see 45 CFR 164.308 (a)(3)).

Implementing policies and procedures for disabling an individual's access to patients' health information through a Health Information Exchange will require coordination with the organization responsible for authorizing the individual under Principle 1.2. Also, disabling a provider's access to patients' health information must be done in a manner that does not adversely impact patients' care.

Recommended Resources for Further Development:

Health care organizations and Health Information Exchanges may find the following national efforts useful in implementing this principle:

- ASTM E1986-98(2005), "*Standard Guide for Information Access Privileges to Health Information*"
- ASTM E1869-04, "*Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records*"
- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"

- The policies, procedures and experience of other Health Information Exchanges, such as the Indiana Health Information Exchange (IHIE)
- ISO/TS 22600-1:2006, "*Health informatics -- Privilege management and access control -- Part 1: Overview and policy management*"

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- Legal counsel
- Corporate compliance staff
- Health information managers
- IT security and operations staff
- Health care providers and others that need access to patients' health information to accomplish their job functions

Access Control Principle P3.6:

Health Information Exchanges should have policies and procedures for terminating a logged-in individual's session accessing patients' health information due to inactivity within the session.

Discussion and Analysis:

This principle is an adaptation of the HIPAA Security regulation requirement that health care organizations implement procedures that terminate an electronic session after a predetermined time of inactivity (45 CFR 164.312(a)(2)(iii)). Most health care organizations have implemented this principle within their organizations, so this principle simply extends that implementation to Health Information Exchanges. This principle will help to protect patients' health information by minimizing the possibility of information being inappropriately accessed through an unattended computer.

Additional development and refinement of this principle should focus on: 1) determining the appropriate timeframe for a session to time-out; and 2) the information system mechanisms to accomplish the termination of a session.

Recommended Resources for Further Development:

Health Information Exchanges may find the following national efforts useful in implementing this principle:

- The policies, procedures and experience of other Health Information Exchanges, such as the Indiana Health Information Exchange (IHIE)

Recommended Stakeholders for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations staff
- Health care providers and others that need access to patient health information to accomplish their job functions

Auditing Principle P4.1:

All organizations participating in a Health Information Exchange should develop and accept minimum standards for routine auditing of individuals' access to patients' health information through the Health Information Exchange.

Discussion and Analysis:

This principle identifies the auditing of individuals' access to patients' health information through a Health Information Exchange as a significant tool for ensuring the patients' health information is not inappropriately accessed. As noted in the discussion of Principle 3.1, many of the access controls associated with a Health Information Exchange will be behavioral controls. Therefore, an auditing program is critical to verifying compliance with the controls developed to limit/prohibit inappropriate access to patients' health information.

Consumer acceptance and public trust will be crucial factors in the success of any Health Information Exchange. This principle, in conjunction with related principles (e.g., Principle 4.4, Investigation of Inappropriate Access and Principle 3.4, Sanctions), will help to reassure patients that the Health Information Exchange is actively protecting their health information.

This principle is also consistent with the HIPAA Security regulations requirement that health care organizations implement audit controls (see 45 CFR 164.312 (b)).

Recommended Resources for Further Development:

Health care organizations and Health Information Exchanges may find the following national efforts useful in implementing this principle:

- Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.
- ASTM E2147-01, "*Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*"
- Best practices and recommendations from professional organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)
- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations staff
- Health information managers
- Corporate compliance staff

Additionally, it would be beneficial to have professionals experienced in information technology audit issues such as, members of:

- Minnesota Chapter of Information System Audit and Control Association

- Minnesota Chapter of the International Information Systems Forensics Association
- Information System Security Association.

These are the three leading professional organization focusing on information auditing and both have active Minnesota chapters. The Minnesota chapter of the Information System Security Association has an active Healthcare Security Professional Interest Group.

Auditing Principle P4.2:

All organizations participating in a Health Information Exchange should maintain audit logs that document individuals accessing patients' health information. The audit logs should minimally identify: a) the individual accessing the health information; b) the health information being accessed; c) the date and time of the access; and d) all failed log-ins.

Discussion and Analysis:

This principle addresses the first requirement of an auditing program – collecting sufficiently detailed data to facilitate an audit. This principle identifies the minimum data necessary to ensure that an organization can determine:

- Who accessed patients' health information
- What patient information was accessed
- When the patient information was accessed
- Where the patient information was accessed

Depending on the architecture of the Health Information Exchange, it may be possible to log this data at either the organization level or at the Health Information Exchange level. This principle does not specify where or how the data is logged and leaves that decision to the organizations and Health Information Exchange. This principle focuses on what information needs to be collected and used as the foundation for the activities in Principles 4.2 and 4.3.

Recommended Resources for Further Development:

Health care organizations and Health Information Exchanges may find the following national efforts useful in implementing this principle:

- Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.
- ASTM E2147-01, "*Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*"
- Best practices and recommendations from professional organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)
- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations staff
- Health information managers
- Corporate compliance staff

Additionally, it would be beneficial to have professionals experienced in information technology audit issues such as, members of:

- Minnesota Chapter of Information System Audit and Control Association
- Minnesota Chapter of the International Information Systems Forensics Association
- Information System Security Association.

Auditing Principle P4.3:

All organizations participating in a Health Information Exchange should develop and accept: a) the data elements to be maintained and exchanged for auditing individuals' access to patient health information; b) the frequency at which the auditing data will be exchanged between organizations participating in the Health Information Exchange; and c) the minimum retention time of audit logs maintained for auditing individuals' access to patient health information.

Discussion and Analysis:

This principle acknowledges that organizations participating in a Health Information Exchange will need to share information in order to properly conduct routine audits as described in Principle 4.2. Although the exact information an organization would have available for auditing from its own sources would depend on the architecture of the Health Information Exchange, it is anticipated that organizations will need to share information to have all the information needed for an audit. For example, the organization where a patient's health information has been accessed will have recorded:

- who accessed the information
- what information was accessed
- when the information was accessed

However, that organization will not have the following necessary information:

- whether or not the patient whose information was accessed was being seen when the information was accessed
- whether or not the provider accessing the patient's information was scheduled to work when the information was accessed
- if the information that was accessed was relevant to the current treatment of the patient
- why the provider accessing the information may have had a need to access the information

All of these elements may be relevant and necessary to performing an audit. Additionally, this principle calls for setting a minimum retention time of audit logs. This aspect of the principle is needed to account for the fact that individuals' inappropriate access of health information is often

discovered during an investigation of a complaint, rather than through a routine audit. Therefore, this principle anticipates the need to maintain audit logs to facilitate complaint-based auditing.

The 4A Subgroup believes that the organization that is requesting the information through the Health Information Exchange should record the same audit data as the disclosing organization whenever it is possible. The Subgroup noted that technological limitations often prevent the requesting organization from logging such data, however when such limitations do not exist it would be beneficial for the requestor to maintain the same audit data.

Recommended Resources for Further Development:

Health care organizations and Health Information Exchanges may find the following national efforts useful in implementing this principle:

- Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.
- ASTM E2147-01, "*Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*"
- Integrating the Healthcare Enterprise (IHE) and their work on audit trails and node authentication
- Information Systems Audit and Control Association and their CobiT project, "*Control Objectives for Informational and Related Technology*"
- The policies, procedures and experience of other Health Information Exchanges

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations staff
- Health information managers
- Corporate compliance staff

Additionally, it would be beneficial to have professionals experienced in information technology audit issues such as, members of:

- Minnesota Chapter of Information System Audit and Control Association
- Minnesota Chapter of the International Information Systems Forensics Association
- Information System Security Association
- Healthcare Information and Management Systems Society (HIMSS).

Auditing Principle P4.4:

All organizations participating in a Health Information Exchange should develop and accept procedures for: a) alerting other participating organizations of situations where patients' health information may have been inappropriately accessed; and b) jointly investigating situations where patients' health information may have been inappropriately accessed.

Discussion and Analysis:

This principle describes the responsibility of organizations participating in a Health Information Exchange to notify other participating organizations if there is evidence or concern that patients' health information may have been inappropriately accessed. There are a number of important reasons for developing procedures to alert other participating organizations of potentially inappropriate access:

- The organizations will be able to share specific information necessary for a complete investigation of the concern.
- All organizations have a responsibility to protect the confidentiality of their patients' data and should be alerted of any situation which may negatively impact their patients' privacy.
- Alerting other participating organizations of potential concerns will allow the organizations to identify, investigate, and mitigate systemic vulnerabilities related to the exchange of patients' health information.
- Alerting other participating organizations may help facilitate the implementation of Principles 3.4, Sanctions and Principle 3.5, Disabling Access.

The 4A Subgroup believes that future development and refinement of this principle should include the following issues:

- The confidentiality of audit information and investigations related to the inappropriate access to patients' health information
- The relationship of this principle to legal requirements (e.g., Minnesota Statutes § 325E.61) to notify patients of breach in the security of information systems
- The clarification of any limits on the use of information exchanged for auditing purposes for other non-auditing purposes.

Recommended Resources for Further Development:

Health care organizations and Health Information Exchanges may find the following national efforts useful in implementing this principle:

- ASTM E2147-01, "*Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*"
- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"
- Integrating the Healthcare Enterprise (IHE) and their work on audit trails and node authentication
- The policies, procedures and experience of other Health Information Exchanges

Recommended Experts for Further Development:

Organizations participating in a Health Information Exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations staff
- Health information managers

- Corporate compliance staff
- Legal counsel

Additionally, it would be beneficial to have professionals experienced in information technology audit issues such as, members of:

- Minnesota Chapter of Information System Audit and Control Association
- Minnesota Chapter of the International Information Systems Forensics Association
- Information System Security Association.

CONCLUSIONS

This report documents the Solutions and Implementation Plans Work Group efforts to develop solutions to eliminate or reduce privacy and security barriers to the electronic exchange of health information while preserving and strengthening patient privacy protections.

The Patient Consent Subgroup proposed a number of modifications to Minnesota Statutes § 144.335 to resolve differences between health care providers regarding “when” and “how” patient consent is required to exchange patients’ health information. The potential solutions address nine specific patient consent issues by:

- Defining undefined terms and ambiguous concepts in Minnesota’s patient consent requirements;
- Adding language to clarify the application of Minnesota’s patient consent requirements to new concepts in the electronic exchange of health information; and
- Updating Minnesota’s patient consent requirements to allow mechanisms that facilitate the electronic exchange of patients’ information while respecting the patients’ ability and wishes for controlling their information.

The 4A Subgroup developed a set of 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange that provide a framework for the continued development of Health Information Exchanges. The principles are specific enough to aid organizations’ decisions regarding the formation and implementation of Health Information Exchanges, yet are sufficiently general to be useful as:

- Health Information Exchanges specify their network architectures;
- Existing information technology evolves and new technology is introduced;
- National standards are developed and refined; and
- Health care organizations gain experience in implementing the electronic exchange of health information.

The efforts of these Subgroups will help to eliminate or reduce the two most significant privacy and security barriers to the electronic exchange of health information in Minnesota.

The MPSP will continue the on-going work of the project and the two Subgroups, which will yield another interim report (due February 2007) that identifies and describes mechanisms and plans for implementing the solutions outlined in this report. A final project report is anticipated in April, 2007.



APPENDIX A SECURITY TERMS AND DEFINITIONS

The 4A Subgroup identified a number of security terms that are used frequently in discussions of information system security. Therefore the Subgroup compiled the following list of definitions and concepts to ensure that everyone involved in the project was using a common lexicon.

Access Authority – An entity responsible for monitoring and granting access privileges for other authorized entities. *Source – National Institute of Standards and Technology SP 800-57*

Access Control - The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities. *Source – National Institute of Standards and Technology FIPS 201*

Administrative Safeguards - Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. *Source - HIPAA*

Audit – Independent review and examination of records and activities to assess the adequacy of systems controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies and procedures. *Source – National Institute of Standards and Technology SP 800-32*

Audit Data – Chronological record of systems activities to enable the reconstruction and examination of the sequence and events and changes in an event. *Source – National Institute of Standards and Technology SP 800-32*

Audit Trail – A record showing who has accessed an IT system and what operations the user has performed during a given period. *Source – National Institute of Standards and Technology SP 800-47*

Authentication – The basic process of validating that someone is who they claim to be. *Source - HIPAA*

Authentication Factors – The authentication process is usually broken down into several methods of challenge and response. 1. Something you know (account/user name, password, PIN, ID number, etc.); 2. Something you have (token, bank card, driver's license, passport, etc.) & 3. Something you are (biometrics, fingerprint, retina, DNA, signature, etc.).

Authorization – The official management decision to permit access to systems based on the implementation of an agreed-upon set of security controls. *Source – National Institute of Standards and Technology SP 800-37*

Biometric – A physical or behavioral characteristic of a human being. SOURCE SP 800-32

Biometric – A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. *Source - National Institute of Standards and Technology FIPS 201*

Computer Forensics – The practice of gathering, retaining, and analyzing computer-related (audit) data for investigative purposes in a manner that maintains the integrity of the data. *Source – National Institute of Standards and Technology SP 800-61*

Federated Identity Management – The use of agreements, standards and technologies to make identity and entitlements portable across autonomous identity domains. The goal of federation is to enable transparent and secure exchange of identity information to enable disparate systems to interoperate at the security level.

Identity – A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information to make the complete name unique. *Source – National Institute of Standards and Technology SP 800-63*

Identity Proofing – The process of providing sufficient information (e.g., identity history, credentials, documents) to a Registration Authority when attempting to establish an identity. *Source – National Institute of Standards and Technology FIPS 201*

Information security – The protection of information and information systems from unauthorized access use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. *Source – National Institute of Standards and Technology SP 800-53 & FIPS 200*

Password – Confidential authentication information composed of a string of characters. *Source - HIPAA* (A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. *Source – National Institute of Standards and Technology SP 800-63*)

Record Locator Service (RLS) –An electronic index of patient identifying information that directs participants in a Health Information Exchange to the location of patient health records held by providers as defined in section 144.335, subdivision 1(b) and group purchasers as defined in section 62J.06, subdivision 6. *Source – MPSP Patient Consent Subgroup*

Registration Authority (RA) – A trusted entity that establishes and vouches for the identity of a subscriber to a HIE. The RA may be an integral part of a HIE, or it may be independent of a HIE, but it has a relationship to the HIE. *Source – National Institute of Standards and Technology Sp 800-63*

Role-Based Access - Determination that the access of a workforce member to electronic protected health information is appropriate with their role or job function. *Source - HIPAA*

Rule-Based Security Policy – A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes of the subjects requesting access. *Source – National Institute of Standards and Technology SP 800-33*

Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. *Source – National Institute of Standards and Technology SP 800-53 & FIPS 200*

Security Credentialing – The process of reviewing and granting a user the appropriate role-based designation and access rights to specific health information.

Security Incident – Means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *Source - HIPAA*

Security Policy – A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. *Source – National Institute of Standards and Technology FIPS 188*

Single-factor Authentication – This is the process by which only one of the three possible factor types is used to authenticate a person for system access. The three factor types include something you know (e.g. an ID and password or PIN), something you have (e.g. a security fob, smart card, or some other physical object that must be presented to enable access) and something you are (e.g. personal biometric, fingerprint, retina scan, etc.), which is unique.

SNO (Sub-Network Organization) – A SNO is any group of entities (regionally or non-regionally defined) that agree to communicate clinical data with one another using a Record Locator Service (RLS), using shared policies and contractual agreements. A SNO has two sets of interfaces, one internal, which binds its member entities together, and one external, which is where traffic to and from other SNOs and outside entities comes from. *Source - Markle Foundation: Connecting for Health Common Framework*

Treatment Relationship - The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. *Source - HIPAA*

APPENDIX B

HEALTH CARE SECURITY STANDARDS AND DEFINITIONS

- **International Standards Organization (www.iso.org)**
 - *ISO 17799 – Code of Practice for information security*
 - *ISO 27799 – Security Management in health using ISO 17799*
 - *ISO/CD TS 21298 – Health informatics functional and structural roles*
 - *ISO/TS 21091:2005 – Directory services for security, communications and identification of professionals and patients*
 - *ISO/TS 17090-1:2002 – Health informatics – Public Key infrastructure*
 - *ISO 26000 – Standard on Social responsibility (In development – 2008)*
 - *ISO/TS 22600-1:2006, “Health informatics – Privilege management and access control – Part 1: Overview and policy management”*
- **ASTM International (www.astm.org) (All of the following standards are ANSI approved.)**
 - *E1762-95(2003) – Standard guide for electronic authentication of health care information*
 - *E1985-98(2003) – Standards guide for user authentication and authorization*
 - *E1986-98(2005) – Standard guide for information access privileges to health information*
 - *E1869-04 – Standard guide for confidentiality, privacy, access and data security principles for health care including EHRs*
 - *E1988-98 – Standard guide for training of persons who have access to health information*
 - *E2147-01 – Standard specification for audit and disclosure logs for use in health information systems*
- **US Health and Human Services Resources (www.os.dhhs.gov/healthit)**
 - *Office of the National Coordinator for Health Information Technology (ONCHIT – www.hhs.gov/healthit/onc/mission/)*
 - *The Center for Disease Control and Prevention’s site on the Public Health Information Network (www.cdc.gov/phn)*
 - *Healthcare Information Technology Standards Panel (HITSP) of the American National Standards Institute (ANSI)
(http://www.ansi.org/standards_activities/standards_boards_panels/hisb/hitsp.aspx?menuid=3/)*
 - *American Health Information Community (AHIC) – Confidentiality, Privacy & Security Workgroup (www.hhs.gov/healthit/ahic/cps_main.html)*

- *Certification Commission for Healthcare Information Technology (CCHIT) Product Certification* (www.cchit.org)
- *HHS Privacy & Security Activities* (www.hhs.gov/healthit/privacy/)
- *HHS Agency for Healthcare Research and Quality – HISPC project* (www.healthit.ahrq.gov/privacyandsecurity)
- *2nd Nationwide Health Information Network forum: NHIN Security Services* (http://www.hhs.gov/healthit/nhin/forum_oct2006.html)

- **Other resources**

- National Institute of Standards and Technology's Computer Security Resource Center (<http://csrc.nist.gov>) (NIST publishes many security guidelines for federal agencies.)
- Computer Emergency Response Team, a federal funded research and development center at Carnegie Mellon University (www.cert.org)
- Institute of Internal Auditors, It Security (www.theiia.org) Information security auditing
- Information Systems Audit and Control Association, "Control Objectives for Informational and related technology (COBIT)" (www.isaca.org/cobit)
- ISSA's General Accepted Information Security Procedures (www.issa.org) The Minnesota Chapter's Healthcare Security Professional Interest Group (www.mn-issa.org)
- IHE Initiative by HIMSS, ACC & RSNA (www.ihe.net)
- HL7 (www.hl7.org)
- The Liberty Alliance (www.projectliberty.org)
- eHealth Initiative's Technology Working Group (<http://www.ehealthinitiative.org/TechWGMaterials.msp>)
- International Information Systems Forensics Association (www.iifsa.org) The Minnesota chapter (www.mn-isfa.org)
- The Markle Foundation's Connecting for Health Common Framework (www.connectingforhealth.org)
- Healthcare Information and Management Systems Society (www.himss.org)
- The Minnesota chapter (www.himss-mn.org)
- American Health Information Management Association (www.ahima.org) The Minnesota chapter (www.mnhima.org)
- The Public Health Data Standards Consortium (<http://phdatastandards.info/>)