

INTERIM IMPLEMENTATION PLANS REPORT

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

February 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 and implementation activities to reduce or eliminate the privacy and security barriers identified within this project.

**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	3
Solution Generation and Implementation Planning Process	5
Introduction	5
Solutions and Implementation Plans Work Group	5
Summary of Solutions Generated	7
Implementation Plans for Modifications to Patient Consent Requirements	9
Implementation Plans for Principles to Authorize and Authenticate Individuals, Set Access Controls, and Audit in a Health Information Exchange	12
Conclusion	17
Appendix A	
Solutions and Implementation Plans Work Group Members	18
Appendix B	
Solutions and Implementation Plan Work Group Charge	20
Appendix C	
Patient Consent Subgroup Charge	22
Appendix D	
4A Subgroup Charge	24
Appendix E	
General Principles for Authorizing and Authenticating Individuals, Setting Access Controls, and Auditing in a Health Information Exchange	26
Appendix F	
Minnesota Department of Health Proposed Modifications to Minnesota Statutes § 144.335	29

EXECUTIVE SUMMARY

The Minnesota Privacy and Security Project (MPSP) is conducting a systematic and comprehensive review of current laws and practices that impede the efficient, electronic exchange of health data. In previous reports,¹ the MPSP identified, analyzed, and provided solutions to address the most significant privacy and security issues facing organizations in implementing the electronic exchange of health information, which were described as:

- **The implementation of Minnesota's patient consent requirements within a health information exchange.**
- **Operational difficulties in first providing, and then limiting and monitoring external organizations' electronic access to patient data.**

This report provides a preliminary update on the plans and activities for implementing solutions to these barriers.

Implementing solutions that address barriers created by Minnesota's patient consent requirements entails: 1) Selecting specific solutions from the set of possible solutions; 2) Working with the Minnesota Legislature to enact legislation that modifies Minnesota Statutes, § 144.335; and 3) Educating patients and providers about changes to the patient consent requirements.

This report describes the following implementation activities:

- The five criteria used by the Minnesota Department of Health (MDH) to select solutions generated by the project's Patient Consent Subgroup;
- MDH's efforts to work with the 2007 Minnesota Legislature in enacting its proposed set of solutions, and/or considering other solutions advanced for consideration; and
- Four specific mechanisms to disseminate information to patients and providers to assist them in understanding any modifications to Minnesota's patient consent requirements.

Implementing solutions that address barriers to providing, limiting, and monitoring external access to patient data entails: 1) Assisting organizations to incorporate a framework of 19 security principles into their planning and implementation efforts for electronically exchanging health information; and 2) Using an on-going work group with appropriate expertise to continue and further develop the framework created by the 19 security principles.

This report describes ways the MPSP, MDH, the Minnesota e-Health Advisory Committee and existing Health Information Exchanges can use and advance the 19 security principles, such as:

- Incorporating the principles into existing security activities and processes;
- Identifying statewide, collaborative efforts to further refine and develop the principles; and
- Including the principles and their further development into recommendations issued by the Minnesota e-Health Advisory Committee; and
- Integrating the principles into grant programs and technical assistance activities at MDH.

¹ Copies of those reports may be found on the MPSP website at: <http://www.health.state.mn.us/e-health/mpsp/>

BACKGROUND

Purpose and Scope

This report provides a preliminary update on the plans and activities for implementing solutions to the most significant privacy and security barriers impeding the electronic exchange of health information. This report builds on the two previous reports² issued by the Minnesota Privacy and Security Project (MPSP) titled, "*Privacy and Security Barriers to the Electronic Exchange of Health Information*" and "*Interim Report of Solutions to Barriers to the Electronic Exchange of Health Information*."

Barriers to the Electronic Exchange of Health Information

The original premise of the MPSP was that significant variations across organizations' business practices for handling and disclosing health information create significant barriers to exchanging data. However, that premise was not supported by the project's analyses. In general, the project did not find significant variations in business practices across organizations, and most organizational variation identified was not deemed a significant impediment to the appropriate exchange of health information.

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

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

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 in Minnesota Statutes, § 144.335. These differences make it impossible for health care providers to agree on "when" and "how" patient consent is required. Second, the patient consent requirements were designed for paper-based exchanges of information and early electronic data base systems are not conducive to a real-time, automated electronic exchange of information.
2. **Operational difficulties in first providing, and then limiting and monitoring external organizations' electronic access to patient data.** This issue is identified as one general issue, although it is really 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;
 - 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

² Copies of those reports may be found on the MPSP website at: <http://www.health.state.mn.us/e-health/mpsp/>

- d. Mechanisms for coordinated auditing across organizations to identify authorized individuals who inappropriately access health information.

Within the project and this report, the second barrier is generally referred to as the 4A barrier because of the need to address Authorization, Authentication, Access Controls and Auditing.

The formation, development, and implementation of arrangements to electronically exchange health information is in its early stages. Most organizations are still working on identifying general issues and the overall set of activities that need to be addressed. In general, most organizations' efforts are still focused on strategic planning activities and have not yet advanced to operational implementation. Consequently, the privacy and security barriers identified and addressed through the MPSP also tended to be focused on a general strategic level, rather than a specific operational level.

The solutions and implementation plans described and detailed in the MPSP's reports are intended to assist organizations in their strategic planning by:

- Providing a common description and analysis of the most difficult privacy and security barriers facing organizations;
- Creating a framework that helps organizations understand the full scope of activities needed to successfully address the privacy and security barriers, particularly for the 4As; and
- Outlining activities and opportunities for organizations to work collaboratively to advance their efforts beyond strategic planning and closer to operational reality.

The implementation plans described in this report are less detailed than were originally envisioned when the project anticipated addressing specific, detailed business practices for handling and disclosing health information. However, the plans discussed in this report are actually more useful at this point in time because the level of detail is more appropriate for and consistent with the needs of Minnesota's health care organizations as they begin to collaborate to exchange electronic health information. More strategic than prescriptively operational, these implementation plans focus on forums and collaborations that enable organizations to collectively address the mix of legal, technological, and organizational issues they now face.

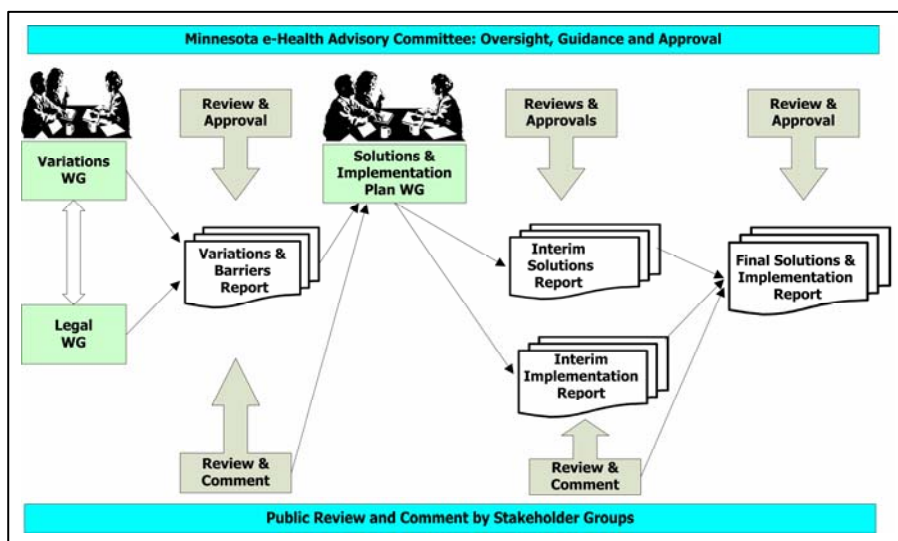
SOLUTION GENERATION AND IMPLEMENTATION PLANNING PROCESS

INTRODUCTION

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 website³. The overall project structure is shown in Figure 1.

The project is under the general guidance of the Minnesota e-Health Advisory Committee⁴, which serves as the steering committee for the project's work. The detailed analytical activities of the project have been carried out through three Work Groups appointed by the MN e-Health Advisory Committee:

Figure 1 – MPSP Structure



the steering committee for the project's work. The detailed analytical activities of the project have been carried out through three Work Groups appointed by the MN e-Health Advisory Committee:

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

SOLUTIONS AND IMPLEMENTATION PLANS WORK GROUP

The solutions and implementation related activities described in this report are a result of the work of the Solutions and Implementation Plan Work Group, which consisted 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;

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

⁴ The Minnesota e-Health Advisory Committee was established by the Governor and the Minnesota Legislature to make recommendations to implement a statewide interoperable health information infrastructure. Information about the Advisory Committee can be found at: <http://www.health.state.mn.us/e-health/advcommittee/>

- 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.

The Solutions and Implementation Plans Work Group was charged with two main 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 the project's initial report.

To meet their charge, the Solutions and Implementation Plans Work Group formed two subgroups to deal with each of the privacy and security barriers individually:

The Patient Consent Subgroup discussed and analyzed potential solutions to address barriers related to Minnesota's patient consent requirements over the course of eight meetings. The two-hour meetings were held between October 18, 2006 and January 17, 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.

The Authorization, Authentication, Access Control and Auditing Subgroup (4A Subgroup) held seven meetings to address the four, inter-related security topics of 1) Authorizing individuals to access patient data; 2) Authenticating individuals when accessing patient data; 3) Setting access controls to appropriately limit authorized individuals' access to patient data; and 4) Coordinating auditing activities across organizations to assure patient data has not been inappropriately accessed. The two-hour meetings were held between October 18, 2006 and January 24, 2007.

Originally, the 4A Subgroup was charged 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.

In addressing its charge, the 4A Subgroup quickly realized that specific policies, procedures, mechanisms or technologies that might serve as solutions would be highly dependent on a number of evolving factors that were outside of the subgroup's control. Therefore, the 4A subgroup developed 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange that would collectively address the mix of legal, technological, and organizational issues faced by organizations. Additionally, the 4A Subgroup identified recommended resources and experts for further developing and refining the principles.

A listing of the Solutions and Implementation Plans Work Group members, including their participation in each of the two Subgroups can be found in Appendix A. The charge to the Work Group and both of the Subgroups can be found in Appendices B - D.

SUMMARY OF SOLUTIONS GENERATED

To understand the implementation activities needed under this project, it is important to understand the types of solutions that were generated, how those solutions address the barriers, and the activities that are both necessary and possible to implement the solutions.

Solutions in the Patient Consent Subgroup

The Patient Consent Subgroup proposed a variety 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 addressed nine specific patient consent issues by:

- Defining undefined terms and ambiguous concepts in Minnesota's patient consent requirements (i.e., Minnesota Statutes, § 144.335);
- Adding new statutory 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 Patient Consent Subgroup generated various potential solutions for each of the nine patient consent issues, and then identified the advantages and disadvantages associated with each of the solutions. The subgroup was only able to reach consensus around specific solutions for one of the nine issues. The inability to reach consensus was not unexpected. Efforts to address patient consent issues have traditionally been contentious with strong emotions on all sides of the issue. Often, the strong differences on patient consent issues have resulted from stakeholders emphasizing different values (e.g., patient privacy, ease of delivering care, administrative burden, etc.) that represent their roles in the health care delivery process. The strength of the Patient Consent Subgroup's work is that it generates a reasonably complete set of possible solutions and provides a description of the advantages and disadvantages, which are agreed upon by stakeholders with differing points of view.

Solutions for barriers created by Minnesota's patient consent requirements all require modifications to Minnesota Statutes, specifically section 144.335. Therefore, **any implementation plan requires enacting**

a law to modify the patient consent requirements. To that end, the Patient Consent Subgroup proposed statutory language to address the following nine issues:

- **Defining undefined terms and ambiguous concepts**
 - Define the term "Health Record."
 - Define the term "Medical Emergency."
 - Define the term "Related Health Care Entity."
 - Clarify the meaning of the term "Current Treatment" in Minnesota Statutes, § 144.335, subdivision 3a (c)(1).
 - Add an exception to patient consent for long term care providers 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.
- **Adding new statutory language to clarify the application of Minnesota's patient consent requirements to new concepts in the electronic exchange of health information**
 - Introduce and define the concept and term "Record Locator Service."
 - Introduce and define the concept and term "Identifying Information."
 - Clarify the appropriate application of the patient consent requirements to a record locator service.
- **Updating Minnesota Statutes, § 144.335 to allow mechanisms that facilitate the electronic exchange of patients' information**
 - Introduce a framework that allows a health care provider to rely on another provider's representation of having obtained patient consent to disclose health records, including a framework to share liability for patient consent between the disclosing and requesting providers.

Solutions in the 4A Subgroup

The 4A Subgroup developed a set of 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange to provide a framework for the continued development of Health Information Exchanges (see Appendix E for a complete listing of the principles). 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 form and 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.

As noted in their charge, the 4A Subgroup originally 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.

The original charge was overly ambitious, because 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 were 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 for the electronic exchange of health information;
- Technology changes to provide enhanced ability to implement technological solutions for 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 general framework of 19 principles for guiding organizations' decisions regarding security issues in the formation and implementation of Health Information Exchanges. To ensure that the 19 principles would be sufficiently general and flexible enough to be applicable for different organizations' unique situations, the principles were developed to be:

- 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 models of Health Information Exchanges.

Implementation activities related to the 4A Subgroup's work will take two forms: 1) Assuring that current security activities are consistent with principles; and 2) Developing and further refining the principles to accommodate the evolving factors described previously. To assist organizations and Health Information Exchanges in using and further developing the 19 principles, the 4A Subgroup identified recommended resources and experts to participate in the development.

IMPLEMENTATION PLANS FOR MODIFICATIONS TO PATIENT CONSENT REQUIREMENTS

A number of activities are required to implement solutions generated by the Patient Consent Subgroup, specifically:

- Selecting a subset of the various solutions generated;
- Developing and introducing legislation to modify Minnesota Statutes, § 144.335 for consideration by the Minnesota Legislature;

- Passing legislation to address the barriers created by Minnesota's patient consent requirements; and
- Educating patients and providers about any changes in Minnesota's patient consent requirements.

Selecting a Subset of Solutions

The Patient Consent Subgroup did not reach consensus on a single set of solutions to modify Minnesota's statutory requirements. Therefore in an effort to advance a set of solutions, the Minnesota Department of Health developed criteria to evaluate and select a set of solutions that would form the basis for proposed legislation. The criteria for selecting between the Patient Consent Subgroup's solutions are presented in order of importance:

- Solutions should maintain or strengthen patients' privacy or control over their health records;
- Solutions should improve patient care;
- Solutions should facilitate electronic, real time, automated exchange of health information;
- Solutions should not place an undue administrative burden on the health care industry;
- Solutions should increase the clarity and uniform understanding of the statutory language and consent requirements.

Using these criteria, the Minnesota Department of Health (MDH) was able to select between the Patient Consent Subgroup's various solutions and to decide on the changes to be included in a legislative package. The solutions selected are shown in Appendix F. MDH's goal in using these criteria was to strike a balance between patients' desire for privacy and the need to facilitate the electronic exchange of health information for improved patient care.

It is important to note that other criteria, a different ordering of these criteria, or other decision mechanisms could lead to the selection of significantly different sets of solutions. Because the legislative process is an open, public process, we anticipate that other stakeholders (e.g., privacy advocates, health care industry, etc.) may select other solutions for inclusion in their legislative activities. This project's thoughtful and thorough discussion will undoubtedly be of great assistance to legislators as they will ultimately be tasked with crafting Minnesota's patient consent law by choosing from a smorgasbord of solutions.

Developing and Introducing Legislation

The Minnesota Department of Health is currently taking all of the steps necessary to develop and introduce legislation during the 2007 Minnesota Legislative session. These actions include:

- Preparing legislative language for consideration;
- Meeting with representatives of the Governor's office to discuss the Minnesota Privacy and Security Project, the project goals, and the processes used to develop potential legislative solutions, and the need for legislative action;
- Meeting with key legislative leaders to discuss the Minnesota Privacy and Security Project, the project goals, and the processes used to develop potential legislative solutions, and the need for legislative action; and
- Working with House and Senate leadership to identify authors and the activities needed for the legislation to be considered.

Passing Legislation

The Minnesota Department of Health (MDH) is committed to working closely with the House and Senate authors of patient consent legislation by:

- Providing all necessary technical support and assistance in explaining and discussing the proposed changes;
- Using the work product of the Patient Consent Subgroup to:
 - Explain why the proposed modifications are necessary to eliminate or reduce barriers to the electronic exchange of health information;
 - Identify the advantages and disadvantages of the proposed changes; and
 - Evaluate any potential amendments and modifications to the legislation.
- Identify and coordinate with key stakeholders who can testify in support of the legislation and explain its impact on their organizations and activities.

MDH will work collaboratively with the Minnesota Legislature to ensure that any legislation to modify Minnesota's patient consent requirements benefits from the efforts and deliberations of the Patient Consent Subgroup.

In previous legislative sessions where the Minnesota Legislature considered patient consent and patient privacy issues, the topic has evoked spirited debate and strong emotions on all sides of the issue. The legislation being proposed by MDH is likely to receive significant interest and attention from a variety of stakeholders, many of whom have strongly differing points of view. While the proposed legislation attempts to carefully balance those differing points of view, it may be impossible to bridge the differences and reach a compromise. In the event that it is not possible to reach agreement on modifications to Minnesota's patient consent requirements in the 2007 legislative session, MDH and the Minnesota e-Health Advisory Committee will continue to collaborate with stakeholders to develop a workable compromise that can be advanced in future legislative sessions.

Educating Providers and Patients about Changes

Assuming that it is possible to pass legislation that modifies Minnesota's patient consent requirements, it will be important to educate health care providers and patients about those changes. The MPSP has identified a number of mechanisms to inform affected stakeholders about any changes:

- The MPSP will send out announcements and information to the Minnesota e-Health Advisory Committee's email list of interest parties;
- Privacy and security will be one of the featured topics at the 2007 Minnesota e-Health Summit on June 28, 2007;
- Modifications to patient consent and new provider requirements may also be included as a Pre-Summit Workshop on June 27, 2007; and
- The MPSP will work with trade associations and professional organizations to help publicize any modifications to the patient consent requirements.

The Minnesota e-Health Advisory Committee serves as the steering committee for the MPSP. This committee was established legislatively in 2005 and is comprised of 26 members who represent key stakeholders including an array of health care providers, payers, public health professionals, and consumers. The 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. In an effort to keep stakeholders informed of the e-Health Advisory Committee's work and activities, the Committee maintains an email list of over 900 interested stakeholder subscribers. The MPSP plans to use this email list to distribute information and announcements that explain any modifications to Minnesota's patient consent requirements that come out of the 2007 legislative session.

Another mechanism that the Minnesota e-Health Advisory Committee has used to bring the community together to discuss issues related to electronic health records and the electronic exchange of health information is an annual, day-long e-Health Summit. The third annual Minnesota e-Health Summit is scheduled for June 28, 2007, and is expected to once again attract over 400 participants. One of the featured topics at this year's event will be privacy and security issues. The program will feature speakers that will discuss national efforts (e.g., AHIC, the State Alliance for e-Health, and other ONC-funded activities). The program will also present the work of the Minnesota Privacy and Security Project as well as other state efforts (e.g., the Minnesota Health Care Connection). Any modifications to Minnesota's patient consent requirements will be prominently featured in the Summit's program to:

- Assist providers in understanding any new responsibilities or requirements associated with the changes;
- Help patients and consumers to understand how the modifications impact their privacy; and
- Discuss how the changes facilitate the electronic exchange of health information.

Also associated with the Minnesota e-Health Summit is a collection of Pre-Summit Workshops that serve as "how to" training opportunities for stakeholders. As part of the planning process for the Workshops, we are examining the feasibility of offering a Patient Consent Workshop to help providers understand the full ramifications of any changes in Minnesota law. The Summit planning committee is currently exploring the possibility of jointly presenting a program with a professional association such as the Minnesota Health Information Management Association (MHIMA), whose members actively participated in the MPSP and have spent many years working on patient consent issues. The benefit of presenting at both the Summit and a Pre-Summit Workshop is that the combination of programs will provide practical information and tools that aid providers in incorporating new patient consent requirements into their daily practices.

MDH and the MPSP will also work with trade associations and professional organizations to provide practical information and tools to aid providers in understanding changes in the patient consent requirements. Many trade associations have participated in the MPSP (e.g., Minnesota Hospital Association, Minnesota Medical Association, and Minnesota Health and Housing Alliance). All of these organizations have a strong interest in helping their member organizations learn about and comply with any modifications to Minnesota law. Given the active participation these organizations brought to the MPSP, we are confident that we can work together to help communicate changes that result from the process. Likewise, we will work with the Minnesota Health Information Management Association and other professional associations whose members are directly responsible for implementing consent requirements into their daily work activities.

IMPLEMENTATION PLANS FOR PRINCIPLES TO AUTHORIZE AND AUTHENTICATE INDIVIDUALS, SET ACCESS CONTROLS, AND AUDIT IN A HEALTH INFORMATION EXCHANGE

The Solutions and Implementation Plans Work Group's 4A Subgroup believes that its 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in a Health Information

Exchange are as complete as possible given the timeframe available to the MPSP. However as the ever-evolving environment related to the formation and implementation of Health Information Exchanges advances, the 19 principles will also need to be advanced through further development and refinement. Therefore, the 4A Subgroup has identified two distinct types of implementation activities:

- Organizations planning for or implementing the electronic exchange of health information should consider the 19 principles to ensure that their activities are consistent with the principles; and
- An on-going work group with appropriate expertise should be convened to continue and further develop the work products of the Minnesota Privacy and Security Project's 4A Subgroup.

The specific recommendation of the 4A Subgroup for continuing their efforts is presented below:

4A Subgroup Recommendation

In order to further advance the work of the 4A Subgroup and to more fully develop the concepts embodied in the document "General Principles for Authorizing and Authenticating Individuals, Setting Access Controls, and Auditing in a Health Information Exchange," an on-going work group of appropriate expertise should be convened to continue and further develop the work products of the Minnesota Privacy and Security Project's 4A Subgroup:

Work Group Activities

The work group should further refine the work of the 4A Subgroup to address and include:

- 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 health information exchanges;
- Technological changes that provide enhanced ability to implement technology solutions to the issues identified by the 4A Subgroup;
- Common and emerging issues that are identified as organizations participating in health information exchanges gain experience in implementing exchanges; and
- "Best practices" and "lessons learned" from other industries implementing e-commerce and information exchanges.

Work Group Members

The work group should be open to organizations and individuals that have an interest in constructively contributing to addressing the issues identified by the 4A Subgroup. Depending on the issues that are addressed, there will be a need to have expertise in:

- Information technology and information system security;
- Health care informatics and health information management;
- Legal issues related to the privacy and security of health information; and
- Human resources issues related to policy development, employee training, and sanction policies.

Working with Other Stakeholders

Many other groups and associations are working on various aspects of the issues identified by the 4A Subgroup. The on-going work group should work collaboratively with these other efforts to ensure that its work is consistent with other community efforts.

To help organizations prioritize their work around the 19 principles, the 4A Subgroup prioritized the principles and selected those that most need further refining for use by organizations in the formation and implementation of a Health Information Exchange. The results of that prioritization process clearly identified four principles for immediate focus. The four principles selected as most critical to the electronic exchange of health information are: (highest priority first)

- 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.
- 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.
- 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.

There are a number of mechanisms that the MPSP, the Minnesota Department of Health, the Minnesota e-Health Advisory Committee, and existing Health Information Exchanges can use to move forward both the 4A Subgroup's specific recommendation of refining the overall framework and to incorporate the principles in ongoing security activities, for example:

- Health Information Exchanges can incorporate the 19 principles into their efforts to plan, implement and evaluate their security processes;
- The Minnesota Health Care Connection (MnHCC) can collaborate with Health Information Exchanges in refining and incorporating the principles in a statewide, consistent manner;
- The Minnesota e-Health Advisory Committee can incorporate the 19 principles and the community's further development of the security framework into its recommendations for a statewide implementation plan; and
- The Minnesota Department of Health can incorporate the 19 principles into its technical assistance and grant programs focused on advancing of e-health.

Incorporating the Principles in Health Information Exchanges

Many of Minnesota's Health Information Exchanges are currently planning for or attempting to implement security measures into their exchange of health information. Many of the details for those security measures

will depend on issues unique to each Health Information Exchange. However, the framework developed by the 4A Subgroup provides guidance on dealing with a number of the most difficult security issues. Additionally, the resources identified by the 4A Subgroup direct organizations to information and tools that allow Health Information Exchanges to develop tailored solutions to their specific security concerns while still being consistent with the overall framework created by the principles.

Several members of the 4A Subgroup represented existing Health Information Exchanges. Many of these individuals plan to use the subgroup's work in their on-going efforts. For example, one Health Information Exchange project is using the 4A Subgroup's principles in developing the contractual arrangement between the participants in the exchange. Likewise, the same exchange is considering using the prioritized principles as the framework for guiding its security planning.

As Health Information Exchanges refine the principles and implement specific security solutions, it will be important to share their information and experience with other organizations looking to electronically exchange health information. There are three specific mechanisms that have been identified for communicating and sharing information about security solutions related to the principles.

- The 2007 e-Health Summit, scheduled for June 28, 2007 will have privacy and security as one of its featured topics. A number of sessions at this event will allow Health Information Exchanges the opportunity to share their efforts in using the principles to develop and implement security solutions;
- The Minnesota E-Health Advisory Committee maintains a list of e-health projects and activities occurring in Minnesota. This list serves as a resource to organizations looking to learn from other organizations' experiences; and
- Minnesota is in the process of forming the Minnesota Health Care Connection (MnHCC), a private-public, not-for-profit collaborative that will interconnect stakeholders for the purpose of electronically exchanging accurate, standardized health information in a secure manner. This new collaborative has the potential to serve as the central point for sharing and coordinating information, experiences, and efforts related to the development and implementation of Health Information Exchanges.

Refining and Developing the Principles at MnHCC

The Minnesota Health Care Connection (MnHCC) is a private-public, not-for-profit collaborative that will interconnect stakeholders for the purpose of electronically exchanging accurate, standardized health information in a secure manner. Some of the many roles that MnHCC has defined for itself include:

- Incrementally building a statewide information exchange;
- Facilitating creation of common governance, process, technology, and other elements;
- Helping organizers of local and regional data exchange efforts; and
- Ensuring that Minnesota's data exchange projects are consistent with national technology platforms and networks.

MnHCC anticipates that it will accomplish these functions by:

- Convening stakeholders to coordinate and assist them in addressing common issues;
- Communicating knowledge to organizations that want to electronically exchange health information;

- Educating and advocating for stakeholders;
- Assessing needs, conducting analysis and carrying out applied research to assist stakeholders.

Although the exact activities and work plans for MnHCC have not yet been developed, the collaborative is willing to consider including further refinement of some of the principles in its activities. Many members of the Minnesota e-Health Advisory Committee – the steering committee for the MPSP – have participated in the formation of the MnHCC. Additionally, the MPSP has worked with key stakeholders to keep MnHCC informed of the project's work and opportunities for continuing select aspects of the project's work after MnHCC is fully formed. The MPSP project director is currently a member of the MnHCC Board of Directors and will work with the collaborative to find an appropriate role for advancing the work of the of the 4A Subgroup.

Incorporating the Principles into Advisory Committee Recommendations

The Minnesota e-Health Advisory Committee is charged by Minnesota Statutes, § 62J.495 with the responsibility of making recommendations for implementing a statewide interoperable health information infrastructure, including recommendations on:

- Estimates of necessary resources;
- Standards for administrative data exchange;
- Clinical support programs;
- Patient privacy requirements; and
- The maintenance of the security and confidentiality of individual patient data.

The 19 principles developed by the 4A Subgroup will form the basis for any recommendations issued related to the authorizing and authenticating individuals, setting access controls, and auditing in a health information exchange.

Incorporating the Principles into Technical Assistance and Grants

In 2006, Governor Pawlenty and the Minnesota Legislature established an interoperable electronic health records grants program for rural and medically underserved areas (Minnesota Statutes, § 144.3345). The grant program was funded with \$1.5 million of one-time funding. In 2007, the Governor's budget proposes \$29.5 million in funding over a three-year period. Within the Governor's proposal, \$750,000 per year is proposed for technical assistance and support to grantees.

The Minnesota Department of Health (MDH) is charged with the responsibility of administering the interoperable electronic health records grants program and providing technical assistance and support to grantees. If the grant program is funded, MDH will promote the use of the MPSP's 19 principles and overall security framework in at least two ways:

- Assisting the grantees in considering the principles as they develop security measures for the electronic exchange of health information; and
- Requiring that any security measures implemented by grantees are consistent with the principles.

Because the interoperable electronic health records grants program focuses on rural and medically underserved areas, many of the grantees have limited familiarity with national and state activities related to privacy and security. Nonetheless, the grantees fully appreciate the importance of adequately protecting and assuring the privacy and security of their patients' health information. Many of the grantees are looking for any practical guidance that can help them in implementing security measures to protect the confidentiality of

their patients' data. As part of the technical assistance and support activities associated with the grant program, MDH will help grantees to understand how the 19 principles provide a framework for guiding and assisting in their decision process.

Likewise, MDH can serve as a bridge between groups working on refining the 19 principles (e.g., MnHCC and large metropolitan Health Information Exchanges) and the grantees. By working with grantees to understand the on-going efforts of MnHCC and other Health Information Exchanges in further developing the 19 principles, MDH will help to create a common, coherent security framework across all Health Information Exchanges in the state, regardless of size or location.

CONCLUSION

This report identifies activities and actions for advancing and utilizing the work of the MPSP to address the two most significant privacy and security barriers impeding the electronic exchange of health information. The implementation activities described in this report will:

- Reduce privacy barriers caused by Minnesota's patient consent requirements by enacting legislation that:
 - Creates uniformity between providers in determining "when" and "how" patient consent is needed to exchange information;
 - Clarifies how patient consent requirements apply to new concepts in the electronic exchange of health information (e.g., record locator service); and
 - Provides new legal mechanisms for facilitating the inclusion of patient consent requirements into electronic exchanges of health information.
- Reduce security barriers related to authorizing and authenticating individuals, setting access controls, and auditing in a Health Information Exchange by:
 - Incorporating the 19 security principles into organizations' on-going planning and implementation activities; and
 - Using existing, collaborative efforts and organizations to further develop the 19 principles in response to the rapidly changing environment of health information exchange.

In conclusion, the MPSP determined that many privacy and security issues arise not because organizations have different practices around the issues. Rather, they are an impediment because organizations have not found any fully adequate mechanisms to address the issues. The implementation plans described in this report are less detailed than were originally envisioned when the project anticipated addressing specific, detailed business practices for handling and disclosing health information.

More strategic than prescriptively operational, these implementation plans focus on forums and collaborations that enable organizations to collectively address the mix of legal, technological, and organizational issues they now face. Nonetheless, we believe that the solutions and implementation plans set forth in this report are real, practical steps toward development of those mechanisms that will relieve liability concerns and enable organizations to reach the full potential of electronically exchanging health information to improve the quality of healthcare while preserving and strengthening patient privacy protections.

APPENDIX A SOLUTIONS AND IMPLEMENTATION PLANS WORK GROUP MEMBERS

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 Solutions and Implementation Plans Work Group and the subgroup meetings. These participants' input and analysis has been critical to accomplishing the goals of the project and in identifying and evaluating potential solutions to the privacy and security barriers impeding the electronic exchange of health information. The members of the Work Group and each of the two Subgroups are identified in the following table:

Solutions and Implementation Plans Work Group		
Patient Consent Subgroup Members *		
Laurie	Beyer-Kropuenske	Minnesota Department of Administration - Subgroup, Co-Chair
Billie	Zippel	Blue Cross and Blue Shield of Minnesota - Subgroup, Co-Chair
Patricia	Carter	HealthPartners
Lois	Dahl	Fairview Health Services
Deb	DeBruin	University of Minnesota Center for Bioethics
Mike	DeWane	Rx2000 Institute
Katie	Engler	Minnesota Department of Administration
Lisa	Fink	Legal Services Advocacy Project
James	Golden	Minnesota Department of Health
John	Gross	Minnesota Department of Commerce
Reidun	Hanson	Hennepin County Medical Center
Dave	Honan	Minnesota Department of Human Services
Eric	Klavetter	Mayo Clinic
Rich	Neumeister	Privacy Advocate
Dave	Orren	Minnesota Department of Health
Julie	Ring	Local Public Health Association
Dan	Routhe	University of Minnesota
Tess	Settergren	St. Mary's/Duluth Clinic Health System
Darrell	Shreve	Minnesota Health and Housing Alliance
Janet	Silversmith	Minnesota Medical Association
Beth	Spohn	Fredrikson & Byron, P.A.
Mark	Sonneborn	Minnesota Hospital Association
Karolyn	Stirewalt	Minnesota Medical Association
Mike	Thorsen	Rx2000 Institute
Todd	Vollmers	Minnesota Department of Commerce

Christina	Wen	Minnesota Department of Health
LaVonne	Wieland	HealthEast Care System
Barb	Wills	Minnesota Department of Health
4A Subgroup Members *		
Greg	Jonsen	HealthPartners - Subgroup, Co-Chair
Greg	Linden	StratisHealth - Subgroup, Co-Chair
Tom	Baden	Minnesota Department of Human Services
Miaja	Cassidy	Medica
Mike	DeWane	Rx2000 Institute
Katie	Engler	Minnesota Department of Administration
James	Golden	Minnesota Department of Health
Tom	Ihlenfeldt	UCare Minnesota
Steve	Jensen	Blue Cross and Blue Shield of Minnesota
Mike	Kongsjord	SISU
Diane	Larson	St. Luke's Hospital
Melinda	Machones	College of St. Scholastica
Ron	McKinnon	St. Mary's/Duluth Clinic Health System
Lee	Olson	Mayo Clinic
Darlene	Pozanc	Community Memorial Hospital
Tom	Reineke	Gillette Children's Speciality Healthcare
Dan	Routhe	University of Minnesota
Christina	Stephens	University of Minnesota
Karolyn	Stirewalt	Minnesota Medical Association
Mike	Thorsen	Rx2000 Institute
Janice	Turek	Winona Health
Christina	Wen	Minnesota Department of Health
Barb	Wills	Minnesota Department of Health
* Participation in the process does not constitute an endorsement of the report or the project's findings.		

APPENDIX B

SOLUTIONS AND IMPLEMENTATION PLAN WORK GROUP CHARGE

Purpose

The Solution/Implementation Plan Work Group will identify and evaluate solutions and implementation activities that:

- Eliminate privacy/security barriers to the appropriate electronic exchange of health information;
- Provide health care organizations flexibility in implementing mechanisms for the appropriate electronic exchange of health information; and
- Maintain and provide appropriate privacy and security protections for individuals' health information.

Membership

The Solution/Implementation Plan Work Group will consist of approximately 40 privacy and security experts representing consumers, health systems, health plans, hospitals, public health agencies, tribal clinics and other organizations involved in the exchange of health information. The privacy and security experts will provide representation in three broad areas:

1. The development and implementation of privacy policies and procedures that protect the privacy and patient rights associated with health information;
2. Information system development and the implementation of security policies and procedures addressing the confidentiality, integrity and availability of health information; and
3. Consumer and patient advocacy.

Approach

The Solution/Implementation Plan Work Group will identify and evaluate solutions that address the barriers documented in the Variations and Legal Work Groups' report titled, "*Privacy and Security Barriers to the Electronic Exchange of Health Information*," focusing primarily on:

- Implementing Minnesota patient consent requirements into electronic health information exchange;
- Ensuring that all parties involved in the electronic exchange of health information share responsibility/liability for the appropriateness of the exchange; and
- Developing a health information exchange framework for authenticating users and controlling access to individuals' health information.

The Work Group will divide into two subgroups: 1) Patient Consent Subgroup; and 2) Authentication and Access Control Subgroup. The Patient Consent Subgroup will address the legal and operational issues of patient consent and organizations' responsibilities for ensuring the appropriateness of information exchange. The Authentication and Access Control Subgroup will address issues related to user authentication and information access controls.

Work Group Charge

The charge of the work group is to:

1. Identify and develop solutions to reduce or eliminate the privacy/security barriers identified by the Variations and Legal Work Groups;
2. Evaluate proposed solutions by assessing:
 - o The relationship of the solutions to the vision, focus and strategic goals of the Minnesota e-Health Advisory Committee;
 - o The impact of the solutions on consumer protection and privacy;
 - o The impact of the solutions on health care organizations' operations and resources;
 - o The relationship of the solutions to national standards.
3. Develop implementation plans that delineate activities necessary for advancing solutions by:
 - o Describing and prioritizing the actions to be taken;
 - o Identifying the organizations and groups responsible for executing the actions;
 - o Outlining the resources necessary to carry out the activities; and
 - o Developing a timeframe for implementing the solutions.
4. Create a Solutions and Implementation Plans Report that documents the work group's reviews and evaluations.

Expectations

1. To bring the perspective of the sector or stakeholders you represent to the work group discussions and decisions;
2. To keep the statewide interests of e-Health foremost in your reviews and evaluations;
3. To work toward solutions and implementation plans that achieve that e-Health Advisory Committee's Consumer Benefit Statements;
4. To review meeting materials ahead of time and be prepared to contribute clear and focused ideas for work group discussion; and
5. To attend meetings (or send an alternate) and participate in conference calls, alerting staff and the chairs ahead of time to any scheduled absence.

APPENDIX C PATIENT CONSENT SUBGROUP CHARGE

Subgroup Charge:

The Patient Consent Subgroup is charged with 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.

Activities Based on Barriers Report:

The *Privacy and Security Barriers to the Electronic Exchange of Health Information* report identified a number of terms that need to be defined or clarified to ensure uniform implementation of the patient privacy protections in M.S. § 144.335. Specifically, the report identified the need to:

1. Define the term "Health Record" – including whether or not demographic data are a health record.
2. Define the term "Medical Emergency."
3. Define the term "Related Health Care Entities."
4. Define or clarify the term "Current Treatment."
5. Depending on the definition of "Health Record," there may be a need to address the expiration period for a patient consent to include demographic data and a pointer to health records in a record locator service.
6. Identify a framework and mechanisms that permit a provider to rely on another provider's representations of having obtained consent – including the transfer of liability.
7. Depending on the definitions and changes, there may be a need to address consumer education issues.

In addition to the activities identified in the report, there may be a need to address other issues depending on the solutions generated for the barriers. Specifically, the group might want or need to:

- Define the term "Record Locator Service."
- Define the term "Demographic Data."
- Define the term "Continuity of Care" – depending on the clarification of "Current Treatment."
- Identify the requirements of patient consent beyond signed, written and dated.
- Define the term "Informed Consent."

Process:

There are multiple options for defining and clarifying each of the terms or requirements. Our goal will be to:

1. Identify a limited number of options for each term or requirement.
2. Identify the advantages and disadvantages of each option.
3. Connect related options into a consistent coherent package of options.
4. Identify any issues associated with implementing various options that need to be considered.
5. Find consensus on options – when possible.

APPENDIX D 4A SUBGROUP CHARGE

Subgroup Charge:

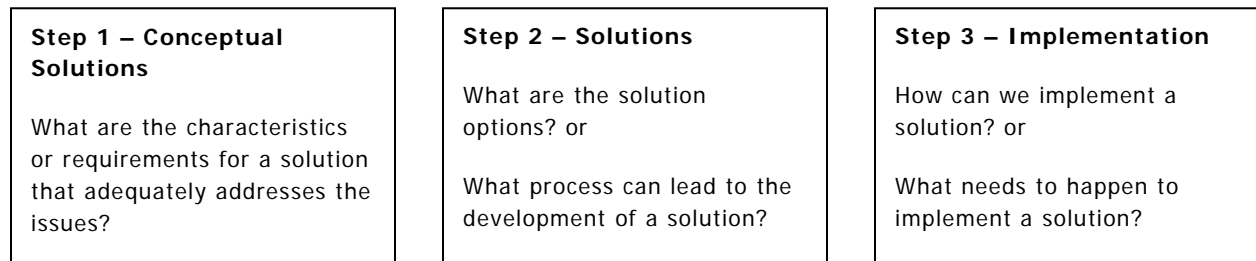
The AAAA Subgroup is charged with identifying solutions or processes for developing solutions that eliminate or reduce barriers to:

1. authorizing and authenticating users within a health information exchange; and
2. limiting and auditing authorized users' access to individuals' health information within a health information exchange.

Issues:

- | | |
|-------------------------|------------------------|
| Authorizing Users | Authenticating Users |
| Setting Access Controls | Auditing Users' Access |

Three Step Process:



Step 1 – Conceptual Solutions:

1. Assumptions Used in Developing a Solution
 - o Definitions
 - o Preconditions
 - o Use Cases
 - o Other Assumptions
2. Principles and Guidelines for a Solution
3. Minimum Functionality or Capabilities of a Solution
 - o Needs a Solution must Address
 - o Minimal Functions a Solution must Include
 - o Data Requirements

Step 2 – Solutions:

1. Options or Solutions
 - Model Policies (Examples or Suggestions)
 - Model Technologies (Examples or Suggestions)
 - Data Requirements
2. Processes or Activities Necessary to Identify a Solution
 - National Activities
 - Process to Reach Agreement

Step 3 – Implementation:

1. How Organizations Move toward Agreement and Implementation
 - Action Steps for Implementation, including Roles and Responsibilities
 - Timeframes for Implementation

APPENDIX E

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

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.

**APPENDIX F
MINNESOTA DEPARTMENT OF HEALTH
PROPOSED MODIFICATIONS TO
MINNESOTA STATUTES § 144.335**

[Information for this Appendix will be added to the report when the proposed modifications are available and introduced at the Minnesota Legislature]

