Privacy and Security Solutions for Interoperable Health Information Exchange

Oregon's Final Implementation Plan Report

Subcontract No. 290-05-0015
RTI Project No. 9825

Prepared by:

Oregon Health Policy and Research
255 Capitol St. NE, 5th Floor
Salem, OR 97310

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

April 16, 2007

OFFICE FOR
OREGON HEALTH
POLICY & RESEARCH

OREGON HEALTH CARE
QUALITY
CORPORATION
A nonprofit partnership for quality improvement

Acknowledgements

The Office of Oregon Health Policy and Research would like to acknowledge the following members of the Oregon Health Information Security and Privacy Collaboration project team for their contributions to this report:

Contributors:

Ree Sailors, MSW Health Policy Advisor
Office of the Governor, State of Oregon Department of Education

Jeanene Smith, MD, MPH Administrator
Office for Oregon Health Policy and Research

Tina Edlund, MS Deputy Administrator
Office for Oregon Health Policy and Research

Jody Pettit, MD, Project Director and Health Information
Technology Coordinator, Office for Oregon Health Policy and Research

Nancy Clarke, Executive Director
Oregon Health Care Quality Corporation

Summer Boslaugh, MBA, MHA Project Manager
Office for Oregon Health Policy and Research

Dawn Bonder, JD Project Manager
Office for Oregon Health Policy and Research

Chris Apgar, CISSP President
Apgar and Associates

Tom Ricciardi, PhD Information Technology Consultant
Oregon Health Care Quality Corporation

&

Steering Committee Members
Work Group Members
The Oregon & SW Washington Healthcare Privacy & Security Forum

I. Background

The electronic exchange of health information holds the potential to revolutionize health care in many ways including through improved quality and cost efficiencies, enhanced patient/consumer engagement, and greater continuity of care. Public trust in health information exchange (HIE) efforts is critical to participation and realization of such benefits. The public must have confidence in the privacy and security protections in place to protect personal health information.

Much of the privacy and security work to date in Oregon has been accomplished by multi-stakeholder groups primarily organized by the hospitals/health systems and the providers through the medical association. Representatives of the State, health plans and others have been active participants over the past 6 years since they assembled to solve issues surrounding the implementation of HIPAA. Another significant background issue is the way in which HIPAA was addressed by the 2003 Oregon Legislature. Prominent privacy and security attorneys and other experts in the state, drawing mainly from the above-mentioned groups examined the relevant state laws and then made sure that they conformed to HIPAA.

The Office for Oregon Health Policy and Research (OHPR) was awarded a contract by RTI, Inc. to participate in the Health Information Security and Privacy Collaboration (HISPC). This Project is part of a national effort managed by the US Department of Health's Office of the National Coordinator for Health Information Technology (ONC), the Agency for Healthcare Research and Quality (AHRQ) and the National Governor's Association. In Oregon the project is a collaboration of OHPR and the Oregon Health Care Quality Corporation. Governor Ted Kulongoski appointed a HISPC Steering Committee with a breadth of expertise and a deep commitment to accomplishing the work of the project. The Steering Committee serves as the decision-making body responsible for the direction of the project, reviewing workgroup products and assuring that all stakeholders' interests are considered.

The Oregon HISPC team engaged a variety of stakeholders to identify and find solutions to the most significant privacy and security issues facing Oregonians with regard to the implementation of the electronic exchange of health information. Broad community input was sought to identify the challenges involved in protecting the privacy and security of health information while enabling electronic HIE and to ensure acceptance of solutions. Many stakeholders from health care, consumer and privacy organizations participated throughout the project.

This report documents the proposed solutions and implementation plan to improve health information exchange in Oregon and the process the project team engaged in to reach the recommendations.

Vision

- Oregonians' health information is available to them and their health care providers anytime, anywhere it is needed.
- Oregonians' health information is private and secure at all times and across all transactions.
- Oregonians' health information is used to assure that personal and population-based health care is safe, effective and efficient.

Mission

To provide guidance regarding laws, principles and best practices that assure the protection of the privacy and security of Oregonians' health information as it is shared electronically across organizations and with individuals in healthcare settings.

Values & Principles

The goal of this effort is to keep Oregonians health information private and secure. The following values frame Oregon's policy for assuring the privacy and security of electronic health information.

- Trust
- Privacy
- Autonomy
- Feasibility
- Balance
- Portability
- Equality
- Transparency
- Public Accountability

The Oregon HISPC project team carefully studied the research on privacy and security of health information exchange in search of a framework apropriate to guide solution recommendations for Oregon. The Markle Foundation's *Connecting for Health* principles regarding the individual and their health information provide such a framework that will allow Oregon to achieve all the solution recommendations detailed in this report. The Steering Committee recognized the importance of the principles in building trust among all parties in Oregon and embraced the principles as the foundation for health information exchange in Oregon.

1. Individuals should be guaranteed access to their own health information.
2. Individuals should be able to access their personally identifiable health information conveniently and affordably.
3. Individuals should have control over whether and how their personally identifiable health information is shared.
4. Individuals should know how their personally identifiable health information may be used and who has access to it.
5. Systems for health information exchange must protect the integrity, security, and confidentiality of an individual's information.
6. The governance and administration of health information exchange networks should be transparent and publicly accountable.

Definitions

To facilitate the policy discussion, definitions of some key terms, taken from the recent Institute of Medicine report, "Disposition of the Air Force Health Study" (2006), are provided below. These definitions were recently referenced in the report submitted to Secretary Michael Leavitt of the US Department of Health and Human Services by the National Committee on Vital and Health Statistics recommending actions regarding "Privacy and Confidentiality in the Nationwide Health Information Network."

Privacy: the right to control the acquisition, uses, or disclosures of his or her identifiable health data.
Confidentiality: the obligations of those who receive information to respect the privacy interests of those to whom the data relate.
Security: the physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

II. Summary of Analysis of Solutions Report

In order to ensure that evolving systems for community-wide exchange of electronic health information adequately protect the privacy and security of individuals, Oregon's public and private partners must work towards the following objectives.

1. **Consumer Protection**
   Adopt the Markle Foundation's Connecting for Health principles regarding the individual and their health information as guiding principles for consumer protection.

   - Individuals should be guaranteed access to their own health information.
   - Individuals should be able to access their personally identifiable health information conveniently and affordably.
   - Individuals should have control over whether and how their personally identifiable health information is shared.
   - Individuals should know how their personally identifiable health information may be used and who has access to it.
   - Systems for health information exchange must protect the integrity, security, and confidentiality of an individual's information.
   - The governance and administration of health information exchange networks should be transparent and publicly accountable.

2. **Provider Identification**
   A coordinated approach to identifying, authenticating and authorizing *providers*

3. **Patient Identification**
   A coordinated approach to identifying, authenticating and authorizing *patients*

4. **Public Engagement**
   An educated and engaged Oregon population regarding health information privacy rights and expectations

5. **Specially Protected Information**
   An examination of state laws that define specially protected health information to determine the appropriateness of the protections and the feasibility of implementing these protections in an electronic environment

6. **Medical Identity Theft**
   An examination of state laws regarding identity theft to determine if medical identity theft is appropriately and adequately addressed

7. **Technical Assistance**
   Support to organizations for comprehensive adoption of appropriate *privacy* and *security* practices for HIPAA and other federal and state law compliance

8. **Non-Covered Entities**
   Legal privacy and security requirements for entities handling personal health information that are not covered by HIPAA

9. **Secondary Use**

An examination of current practices for secondary use of data to determine an acceptable balance between ensuring that personal health information is protected and making de-identified data available for appropriate use

10. **Enforcement**
Legislative or regulatory measures to address inappropriate disclosures and mitigate potential harmful effects of personal health information disclosure

III. Review of State Implementation Planning Process

The planning process for implementation began by engaging the Steering Committee in reviewing and discussing the recommendations developed by the project team. Committee members focused on assigning the most appropriate entity accountability to take the lead on each project as well as potential partners and funding sources. As part of the discussion, members assigned accountability for the solutions to state government, the private sector, federal government, or a partnership of state government and the private sector.

Before convening the Implementation Plan Work Group, the project team expanded the solutions recommendations to incorporate more details about the activities necessary to implement each solution. The team used information gathered in the Solutions Work Group discussions to facilitate this task.

IV. Implementation Plan

Statewide Strategy Coordination

In order to ensure that evolving electronic health information systems adequately protect the privacy and security of individuals, Oregon's State leadership must coordinate the solutions identified in this plan. To achieve this the Oregon HISPC Team recommends following:

- Establish a Health Information Privacy and Security Advisory Board to advise the State regarding privacy and security
- Convene a statewide consortia comprised of representatives from each community exchange to foster and ensure consistency of approach to protecting privacy and security across Oregon
- Provide recommendations to state legislators and policy makers through analysis, briefings and testimony
- Track and participate in the national discussion on HIE privacy and security issues to assure Oregon methods will align with national initiatives
- Provide coordination for government programs that interface with the private sector
- Staff a fulltime HI Privacy and Security position to be housed in the Office for Oregon Health Policy and Research, including staffing and program funds

Implementation Plans for Identified Solutions

Throughout the implementation planning process the project team and the Steering Committee have focused on building consensus and buy-in; everyone feels strongly that it is preferable to solidify this support as we move forward to ensure successful implementation in the future. For this reason we have focused our efforts on developing robust implementation plans for three of the ten solutions. Table 1 describes all ten of the solutions and a detailed implementation plan follows for three of the solutions.

Table 1: Oregon Solutions and Activities to Address Privacy and Security of HIE

Consumer Privacy and Security Protection
Solution: Adopt the Markle Foundation's *Connecting for Health* principles regarding the individual and their health information as guiding principles for consumer protection. 1) Individuals should be guaranteed access to their own health information. 2) Individuals should be able to access their personally identifiable health information conveniently and affordably. 3) Individuals should have control over whether and how their personally identifiable health information is shared. 4) Individuals should know how their personally identifiable health information may be used and who has access to it. 5) Systems for health information exchange must protect the integrity, security, and confidentiality of an individual's information. 6) The governance and administration of health information exchange networks should be transparent and publicly accountable.
Rationale: Consumers must have confidence that HIE efforts will keep their individual health information private and secure. Without consumer trust and acceptance, HIE efforts will be unsuccessful
Coordinating Responsibility: Shared Public-Private partnership

Activities:	Implementers:
Identify appropriate statutory solutions to ensure the Markle principles are implemented in Oregon	Legislature
Implement the Markle principles in HIE policy, architecture, and business agreements	Private sector consortia
Implement the Markle principles in State programs, including PEBB, Medicaid, and state funded HIE pilots	State Government
Implement the Markle principles wherever personal health information is exchanged	Shared Public-Private partnership

Provider Identification

Solution: A coordinated approach to identifying, authenticating and authorizing providers

Rationale: The current approach to provider identification is insufficient for the growing environment of health information sharing across organizations and systems. Improving trust between organizations and developing a common method of identifying, authenticating and authorizing providers is efficient for both the system and the end user. Participants in HIE must be able to know who a provider is, if they are allowed in the system and if they are who they say they are.

Coordinating Responsibility: State Government and Private sector consortia

Activities:	Implementers:
Engage the OMA, OAHHS, OHSU and OBME in the design of a database that authenticates providers based on licensure credentials.	OMA, OAHHS, OHSU, OBME
Develop a standard approach to provider authentication and authorization that uses appropriate and feasible safeguards and technology	Oregon Medical Association and State Government
Engage vendor partners as appropriate	
Participate in national discussion as it evolves	

Patient Identification

Solution: A coordinated approach to identifying, authenticating and authorizing *patients*

Rationale: Accurate identification of patients is essential to matching records across health systems providing quality care. This task is more challenging in the HIE environment as the quantity of patient information and the number of sources of information increases. In addition, the HIE environment makes it possible for the patient to be involved in managing their information. Consistent expectations surrounding how patients should be identified, authenticated, and authorized are necessary to ensure successful matching of patients to their information and to build trust in the system.

Coordinating Responsibility: State Government and Private sector consortia

Activities:	Implementers:
Review and analyze RAND study on patient identifiers	Private Sector Consortia
Review and assess use of Master Person Identifiers (MPIs)	Private Sector Consortia
Evaluate existing systems for patient identification currently used at major provider and payer systems	Private Sector Consortia
Assess the issuance of voluntary patient ID numbers	Private Sector Consortia
Monitor and assess pilot group models	Private Sector Consortia
Adopt or develop a set of common standards or models for identifying patients within and across HIE systems	Private Sector Consortia
Develop a funding strategy to maintain the system	Private Sector Consortia
Assist in communicating needs to vendors and regional	Private Sector Consortia

health information exchanges	
Negotiate bulk purchase rates with vendors	Private Sector Consortia
Public Engagement	
Solution: An educated and engaged Oregon population regarding health information privacy rights and expectations	
Rationale: Consumers are aware of the benefits of HIE but also demonstrate very high levels of concern regarding privacy and security. Engagement of patients must be managed well in order for HIE efforts to succeed. Even one failure in one community could be extremely detrimental to the success of HIE efforts.	
Coordinating Responsibility: Shared Public-Private partnership	
Activities:	**Implementers:**
Develop plain-language HIE privacy and security practice descriptions to be used to inform and educate consumers	Public-Private Partnership
Develop a participation permission form based upon the Markle Foundation *Connecting Health Principles* which incorporates the plain-language privacy and security practice descriptions and test form with consumers to assess understandability of language and concept	Public-Private Partnership
Build statewide consensus on a uniform process for implementing participation permission form	Public-Private Partnership
Develop and build a monitored process to ensure compliance with the uniform process for implementing participation permission forms for all HIE systems	Public-Private Partnership
Specially Protected Information	
Solution: An examination of state laws that define specially protected health information to determine the appropriateness of the protections and the feasibility of implementing these protections in an electronic environment	
Rationale: Many of the laws specially protecting sensitive information were enacted before HIPAA. These laws provide very important protections, but they also present technical difficulties and create interstate barriers that are becoming more significant as our population becomes increasingly mobile and delivery systems grow across state lines.	
Coordinating Responsibility: State government, with private partners	
Activities:	**Implementers:**
Create or engage an entity that can engage and educate consumers about the issue.	
Publish consumer-level explanations of the current laws & rules protecting privacy	
Develop lists of frequently asked questions (FAQs) or recommendations regarding how consumers may ensure the maximum privacy of our information, while at the same time obtaining needed care as efficiently as possible	
Develop a website with educational information and resources	
Engage in an outreach campaign to promote the materials; for example contact the popular media with illustrative examples of dangers to privacy in health care, and with advice on how consumers may access the resources above.	
Medical Identity Theft	
Solution: An examination of state laws regarding identity theft to determine if medical identity theft is appropriately and adequately addressed	

Rationale: Identity theft legislation is essential to regulate inappropriate disclosures of personal health information, including actions taken to prevent such disclosures and actions taken after such disclosures have occurred. Identity theft in a health care setting involves the additional risk of false and erroneous information becoming part of victims' health records. The need to prevent inappropriate disclosures and identity theft is even greater in an HIE environment due to increased possibility of breaches.	
Coordinating Responsibility: State government, with private partners	
Activities:	**Implementers:**
Monitor laws and administrative rules developed to ensure medical identity theft is addressed	State Advisory Board, State Government, Private Partners
Make recommendations to DCBS on laws needed	State Advisory Board, State Government, Private Partners
If appropriate, develop materials and recommendations for healthcare providers to educate them of this issue	State Advisory Board, State Government, Private Partners
If appropriate, develop materials and recommendations for consumer education	State Advisory Board, State Government, Private Partners
Coordinate across state agencies, including DCBS, regarding identity theft legislation	State Advisory Board, State Government, Private Partners
Technical Assistance	
Solution: Support to organizations for comprehensive adoption of appropriate *privacy* and *security* practices for HIPAA and other federal and state law compliance and contractual obligations.	
Rationale: Wide variation exists across organizations in Oregon in the understanding and adherence to appropriate privacy and security practices. Recommended practices are rapidly evolving as technological capabilities advance. In addition, organizations that are unprepared and unequipped to appropriately protect health information are becoming involved in electronic information exchange. The HISPC project has developed a list of recommended practices, but an ongoing effort to keep this information up-to-date and sustain its use is necessary to ensure widespread adoption of appropriate privacy and security practices.	
Coordinating Responsibility: Public and private sector consortia	
Activities:	**Implementers:**
Support the Oregon and SW Washington Privacy and Security Forum's and OAHHS' work in this area	Private Sector and State Partnership
Post the best practices on Q-Corp website and distribute across state	Private Sector and State Partnership
Recognize the role of the State, the Forum, and the OAHHS to endorse practices	Private Sector and State Partnership
Implement the endorsed practices	Private Sector and State Partnership
Identify audience and funding to distribute practices	Private Sector and State Partnership
Maintain and update the recommended practices	Private Sector and State Partnership
Support organizations adopting the practices administratively and technologically	Private Sector and State Partnership
Non-Covered Entities	
Solution: Legal privacy and security requirements for entities handling personal health information that are not covered by HIPAA	
Rationale: HIE efforts are creating new entities that handle personal health information. These	

entities are not covered by HIPAA law and the potential for abuse is high. At a minimum, legal standards at a level equivalent to HIPAA need to be enacted to ensure personal health information is protected by these entities. An approach to regulating these entities may have applicability and be appropriate to regulating HIPAA covered entities participating in HIE	
Coordinating Responsibility: State government, with private partners	
Activities:	**Implementers:**
Work in partnership with the Oregon Attorney General, who is a voting member of the State e-Health Alliance and the Oregon Department of Consumer and Business Services to explore options with respect to legal standards for non-HIPAA covered entities. Also engage with, the National Conference of Commissioners on Uniform State Laws, the new president of NCCUSL is in Oregon	State Government
Engage vendors such as Omnimedix, WebMD and other non-covered entities providing consumer personal health information products to work on solutions	State Government, Private Partners
If determined to be necessary and appropriate, develop and implement legislation and regulations to ensure non-covered entities maintain appropriate privacy and security practices	Advisory Board
Secondary Use	
Solution: An examination of current practices for secondary use of data to determine an acceptable balance between ensuring that personal health information is protected and making de-identified data available for appropriate use	
Rationale: Secondary use of data is expected to be a major revenue source for HIE systems. It is critical that secondary use is conducted in ways that protect patients' rights to gain the trust of patients and ensure the success of HIE efforts.	
Coordinating Responsibility: State government, with private partners	
Activities:	**Implementers:**
Identify and define types of secondary use and develop model practices, policies and procedures for each type.	Advisory Board
Provide technical assistance to HIE efforts to aid adoption of appropriate secondary use practices	State Government
Coordinate with Institutional Review Boards to ensure their alignment with models	State Government
Enforcement	
Solution: Legislative or regulatory measures to address inappropriate disclosures and mitigate potential harmful effects of personal health information disclosure	
Rationale: Enforcement today is not adequate and as HIE efforts move forward enforcement will be essential for ensuring appropriate practices and building the trust of participating organizations and individuals.	
Coordinating Responsibility: State government, with private partners	
Activities:	**Implementers:**
Assess current State and Federal law which is being used or not used for enforcement	Advisory Board, Private Partners
Review national model laws and enforcement mechanisms and evaluate applicability of these and current Oregon laws to the HIE environment	Advisory Board, Private Partners
Develop and build a system to assist consumers in	Advisory Board, Private Partners

understanding their rights and the ability to seek redress when those rights have been violated	

Individuals' Health Information Privacy Protection

1.1. PLAN TITLE: Implementation of Health Information Privacy Protections for Individuals

1.2. PLAN SUMMARY

1.2.1 BRIEF DESCRIPTION: This effort will focus on adoption of the Markle Foundation's *Connecting for Health* principles regarding individuals and their health information as guiding principles for protection of an individual's privacy. Consumers are aware of the benefits of health information exchange but also demonstrate very high levels of concern regarding privacy and security. Engagement of patients must be managed well in order for HIE efforts to succeed. Even one failure in one community could be extremely detrimental to the success of HIE efforts.

1.2.2 RATIONALE FOR STRONG PRIVACY PROTECTIONS FOR INDIVIDUALS: The Markle Foundation has established principles that outline proposed privacy protections for individuals. This implementation uses these principles as a foundation to guide appropriate privacy protections and address consumer trust issues regarding the electronic exchange of health information. Individuals must have confidence that HIE endeavors will keep their information private and secure. Without the trust and acceptance of individuals, HIE efforts will be unsuccessful.

The Markle Principles

1. Individuals should be guaranteed access to their own health information.
2. Individuals should be able to access their personally identifiable health information conveniently and affordably.
3. Individuals should have control over whether and how their personally identifiable health information is shared.
4. Individuals should know how their personally identifiable health information may be used and who has access to it.
5. Systems for health information exchange must protect the integrity, security, and confidentiality of an individual's information.
6. The governance and administration of health information exchange networks should be transparent and publicly accountable.

1.2.3 LEAD ORGANIZATION: The lead coordinating organization for this implementation plan is a public and private sector consortia currently being formed. The consortia will be responsible for organizing the development of training materials, distribution of identified standards, etc. Also, the consortia will assist in expanding the support and adoption of common practices across the industry and in the public sector.

1.2.4 KEY STAKEHOLDERS AFFECTED: The following organizations, groups of stakeholders and interested parties will be affected by and/or primarily involved in various aspects of the implementation plan.

1.2.4.1. **Oregon Legislature:** The Oregon Legislative Assembly plays a

significant role in crafting public policy and enacting legislation affecting implementation requirements with respect to individual rights related to use and disclosure of protected health information. Also, the Assembly plays a very important role in the allocation of funding to advance individual privacy and security protection as the industry moves towards interoperable health information exchange.

1.2.4.2. **Private Sector Consortia:** The private sector has a strong influence on public policy and on implementation of necessary standards to protect the rights of individuals and to accommodate access to and control of the health information of individuals.

1.2.4.3. **State Government:** State government is often charged with implementing public policy as defined by the Office of the Governor and the Legislative Assembly. Also, state government is responsible for enforcement of public policy adoption in many cases.

1.2.4.4. **Shared Public/Private Partnership:** As opposed to state government alone or a private sector consortium alone, a partnership between the public and private sector represents further movement ensuring adoption of The Markle Principles by balancing business needs with regulatory requirements.

1.3 SCOPE: The scope of this plan includes establishing an environment where individuals have firm confidence that HIE efforts will keep their health information private and secure and provide additional individual control over the use of and access to their health information Actions that will be included in this scope include:

1.3.1 Create an education tool for the public explaining HIE in plain language and offering individuals the opportunity to grant permission for their information to be exchanged through a HIE. This tool will clearly and accurately describe what information would be shared and who will have access to the shared information. The tool will also explain to individuals that denial of permission for participating in the HIE may affect the quality of the individual's care and under current HIPAA laws does not prevent other exchanges of health information as allowed (Responsible party: Shared Public/Private Partnership).

1.3.2 Design and implement a process for tracking and honoring the permission form within HIE projects to ensure the request for permission is a meaningful one (Responsible party: Shared Public/Private Partnership).

1.3.3 Design and implement an enforcement mechanism to ensure the assurances made to individuals about the privacy and security of their health information in a HIE can be monitored and violation of assurances will be remedied and appropriate penalties enforced (Responsible parties: Shared Public/Private Partnership and State government, specifically the Oregon Department of Human Services and the Oregon Department of Consumer and Business Services).

1.3.4 Identify appropriate statutory solutions to ensure The Markle Principles are implemented in Oregon (Responsible party: Oregon Legislative Assembly with

stakeholder input)

1.3.5 Implement The Markle Principles in HIE policy, new law (see preceding), architecture and business agreements (Responsible party: Private Sector Consortia with consumer involvement)

1.3.6 Implement the Markle principles in State programs, including the Oregon Public Employee Benefits Board (PEBB), Medicaid, and state funded HIE pilots and enforce new laws established by the Oregon Legislative Assembly relating to the adoption of The Markle Principles as a public good. (Responsible party: State government, specifically the Oregon Department of Human Services and the Oregon Department of Consumer and Business Services).

1.3.7 Implement The Markle Principles wherever personal health information is exchanged (Responsible party: Shared Public/Private Partnership).

1.4 TASKS, TIMELINE AND KEY MILESTONES: A summary of the Individuals' Privacy and Security Protections deliverables in order of their estimated date of completion is included in Table 1:

Table 1. Deliverables: Implementation of Individuals' Privacy and Security Protections for Oregon HIE

PROJECT PLAN REFERENCE	MILESTONES/DELIVERABLES	ESTIMATED COMPLETION DATE
1.3.1	Create an education tool for the public explaining HIE in plain language and offering individuals the opportunity to grant permission for their information to be exchanged through a HIE. This tool will clearly and accurately describe what information would be shared and who will have access to the shared information. The tool will also inform individuals that denial of permission for participating in the HIE could affect the quality of the individual's care and does not prevent other exchanges of health information as allowed under current HIPPA laws	
1.3.2	Design and implement a process for tracking and honoring the permission form within HIE projects to ensure the request for permission is a meaningful one	
1.3.3	Design and implement an enforcement mechanism to ensure the assurances made to individuals about the privacy and security of their health information in a HIE can be monitored and violation of assurances will be remedied and appropriate penalties enforced	
1.3.4	Identify appropriate statutory solutions to ensure the Markle principles are implemented in Oregon	6/30/08

1.3.5	Implement the Markle principles in HIE policy, new law (see preceding), architecture and business agreements	
1.3.6	Implement the Markle principles in State programs, including the Oregon Public Employee Benefits Board (PEBB), Medicaid, and state funded HIE pilots and enforce new laws established by the Oregon Legislative Assembly relating to the adoption of the Markle principles as a public good.	
1.3.7	Implement the Markle principles wherever personal health information is exchanged	

1.5 POSSIBLE BARRIERS: This implementation plan addresses the essential need for significant improvements in the area of providing appropriate security and privacy protections for individuals, increased consumer trust and increased individual control over access and use of their health information. This represents a sound direction and accommodates greater involvement of the consumer in healthcare as well as adequate protections in an HIE environment. Problems arise regarding current available technical standards, system interoperability, culture, etc. Care needs to be taken during the implementation process to address existing issues (especially consumer trust and provider concerns regarding appropriate care based on complete information). Short term milestones can be established however, full implementation is a long term endeavor.

1.5.1 Difficulty in involving consumers in the process of determining what the final rollout of The Markle Principles and actual application should look like.

1.5.2 Complexities in the technical implementation, interoperability issues and the lack of a centralized method of accommodating greater control by individuals over use and disclosure of their health information (which includes the fact that a considerable amount of information is still stored on paper).

1.5.3 Lack of health system consensus on principles of consumer engagement and individual control of records and information.

1.5.4 Logistical challenges given the large population and complexity of the topic.

1.5.5 Tailoring the educational tool for all audiences and reading levels.

1.5.6 Resources for management and carrying out the program.

1.5.7 Discrepancy between HIPAA carve out for payment, treatment and operations and the newer philosophy of individual control.

1.6. OVERALL FEASIBILITY CONSIDERATIONS: Assuming the most significant barriers listed above can be effectively managed; successful implementation of the major activities described in this implementation plan is feasible. Feasibility will be impacted by the

degree of consumer involvement and industry buy-in as well as the availability of funding. Also, successful implementation needs to include broad consumer and healthcare industry education regarding consumer rights, implementation requirements, etc.

Adoption of The Markle Principles which includes rollout of the supporting technical infrastructure needs to be viewed as a long term project. Short term goals include policy maker education, private sector education and engagement and consumer education and engagement. Given appropriate planning and inclusion of interested parties, this implementation plan is presumed to be feasible.

1.7. IMPLICATION FOR IMPLEMENTATION EFFORTS BEYOND STATE BOUNDARIES MULTI-STATE IMPLEMENTATION PLANS

Not applicable for this implementation plan.

NATIONAL-LEVEL RECOMMENDATIONS

The Markle Principles should be closely reviewed by Congress and the US Department of Health and Human Services (HHS). A considerable amount of work went into the development of these principles and it would be valuable to see the adoption of these principles at a national level rather than just at a state level. This would assist in highlighting the importance of these principles and it would assist in moving the healthcare industry forward towards broad adoption of these principles.

1.8. NEXT STEPS

Oregon HISPC has designed a consumer education tool and permission form for health information exchange that will be tested in both the metro area and a rural area. The tool will be revised based upon comments and feedback from interview subjects in both test areas. The revised tool will be vetted with a provider discussion group and a consumer advocate discussion group. The goal is to use this education tool with the pilot HIE projects currently being developed in Oregon. The education tool has been designed with a “modular” concept to allow each HIE to include information that is specific to their project.

Additionally, the project team expects the initial round of interviews to highlight and define areas for further study. We hope to further test the tool with more defined groups, focusing on differences in age, education, ethnicity, income, race and language. A more detailed study of the education tool will allow us to refine the plain language to meet the needs of the diverse population we hope to engage in HIE.

We will continue to work with our stakeholders to design and implement a process for honoring individuals’ wishe concerning participation in a HIE.

Technical Assistance & Sharing Appropriate Practices

1.1. PLAN TITLE: Implementation of Technical Assistance & Sharing Appropriate Practices

1.2. PLAN SUMMARY

1.2.1 BRIEF DESCRIPTION: This effort will focus on implementation of a technical assistance program and education related to appropriate privacy and security practices for HIPAA and other federal and state law compliance and contractual obligations.

1.2.2 NEED TO ADDRESS INCOMPLETE OR INACCURATE KNOWLEDGE IN THE HEALTHCARE INDUSTRY AND PROMULGATE APPROPRIATE PRIVACY AND SECURITY PRACTICES. Wide variation exists across organizations in Oregon in the understanding and adherence to appropriate privacy and security practices. Recommended practices are rapidly evolving as technological capabilities advance. In addition, organizations that are unprepared to adequately protect health information are becoming involved in electronic information exchange. The HISPC project has developed a list of recommended practices, but an ongoing effort to keep this information up-to-date and sustain its use is necessary to ensure widespread adoption of appropriate privacy and security practices.

Also, education is required to assist in dispelling myths or incorrect legal interpretation of existing law that create barriers to health information exchange. The communication of standardized approaches needs to be accompanied with the rationale behind those standards, correct information regarding legal requirements and how misinformation and incomplete adoption of appropriate privacy and security standards hampers quality healthcare while also diminishing the trust of consumers.

1.2.2.1.	Privacy and security standards developed as part of the Oregon HISPC project need to be communicated to the Oregon healthcare industry and to consumers.
1.2.2.2.	Standards need to be flexible and take into account outcomes from the HITSP and other related projects with any modifications communicated to Oregon's healthcare community in a timely manner.
1.2.2.3.	Education programs need to be developed and implemented that provide technical assistance; assist in developing and implementing appropriate privacy and security policies, procedures and practices; and provide an on-going mechanism to address questions that arise as the industry moves forward towards greater adoption of electronic health information exchange and adoption of privacy and security practices.
1.2.2.4.	Communication must include educational material regarding security as much more than a set of technical requirements.

1.2.2.5.	Standards communication needs to address development of templates (e.g., contracts, business associate contracts, consent forms, authorization forms, notices of privacy practices, etc.)
1.2.2.6	A technical and educational advisory body needs to be formed to address on-going issues, continued education and changes in standards.

1.2.3 LEAD ORGANIZATION: The lead coordinating organization for this implementation plan is a currently being formed public and private sector consortia. The consortia will be responsible for organizing the development of training materials, distribution of identified standards, etc. Also, the consortia will assist in expanding the support and adoption of common practices across the industry and in the public sector.

1.2.4 KEY STAKEHOLDERS AFFECTED: The following organizations, groups of stakeholders and interested parties will be affected by and/or primarily involved in various aspects of the implementation plan.

1.2.4.1. **Private Sector and State Partnership:** Oregon state government and private industry play an important part in developing a much needed partnership that assists with the development of technical assistance documentation, validation of standards, development of educational material, etc. Given the solution addressed through this implementation plan crosses the boundary between government and the private sector, close partnership is required to reasonably ensure the program is successful and that government and private industry buy-in is obtained as early in the process as possible.

1.3. SCOPE: The scope of this plan includes formal adoption of appropriate security and privacy standards that address regulatory compliance, appropriate business practices and assist the industry in limiting liability through a general adoption of standards that is adhered to across the industry. This includes the need for education, idea sharing, development of effective training material, training implementation, continued availability of standards and educational material (as well as potentially a source to address specific organization level questions) and on-going standard and educational material maintenance and update. The scope of this implementation plan includes:

1.3.1 Support the Oregon and SW Washington Healthcare, Privacy and Security Forum's (the Forum) and Oregon Association of Hospitals and Health Systems' (OAHHS) work in this area

1.3.2 Post defined appropriate practices on the Oregon Healthcare Quality Corporation (Q-Corp) and the Forum websites and distribute across state

1.3.3 Recognize the role of the State, the Forum, and the OAHHS to endorse practices

1.3.4 Identify audience and funding to distribute practices

1.3.5 Implement endorsed practices (administrative, physical, technical and related business)

1.3.6 Maintain and update the recommended practices

1.3.7 Support organizations adopting the practices administratively and technologically

1.3.8 Develop or assist in development of educational materials and distribution methods

1.3.9 Roll out educational programs and technical assistance

1.3.10 Assist in the formation of an on-going body to update educational material and standards as necessary, distribute updates across the public and private sector and potentially form an operational knowledge center that is able to address individual organizations' questions as standards are being implemented and appropriate practices adopted

1.3.11 Develop or assist in development of standard templates (contracts, business associate contracts, notices of privacy practices, etc.) to be adopted by the private and public sector

1.4. TASKS, TIMELINE AND KEY MILESTONES: A summary of the Technical Assistance and Sharing Appropriate Practices deliverables in order of their estimated date of completion is included in Table 1:

Table 1. Deliverables: Implementation of Technical Assistance and Sharing Appropriate Practices for Oregon HIE

PROJECT PLAN REFERENCE	MILESTONES/DELIVERABLES	ESTIMATED COMPLETION DATE
1.3.1	Support the Oregon and SW Washington Healthcare, Privacy and Security Forum's (the Forum) and Oregon Association of Hospitals and Health Systems' (OAHHS) work in this area	On-going
1.3.2	Post defined appropriate practices on the Oregon Healthcare Quality Corporation (Q-Corp) and the Forum websites and distribute across state	On-going
1.3.3	Recognize the role of the State, the Forum, and the OAHHS to endorse practices	4/30/07
1.3.4	Identify audience and funding to distribute practices	10/1/07
1.3.5	Implement endorsed appropriate practices (administrative, physical, technical and related business)	7/1/08
1.3.6	Maintain and update the recommended practices	On-going

1.3.7	Support organizations adopting the practices administratively and technologically	On-going
1.3.8	Develop or assist in development of appropriate educational materials and distribution methods	7/1/08
1.3.9	Roll out educational programs and technical assistance	1/1/09
1.3.10	Assist in the formation of an on-going body to update educational material and standards as necessary, distribute updates across the public and private sector and potentially form an operational knowledge center that is able to address individual organizations' questions as standards are being implemented and appropriate practices adopted	10/1/08
1.3.11	Develop or assist in development of standard templates (contracts, business associate contracts, notices of privacy practices, etc.) to be adopted by the private and public sector	7/1/08

1.5. POSSIBLE BARRIERS: This implementation plan addresses the essential need for significant improvements in the area of establishing broadly adopted security and privacy standards that are consistently implemented across the healthcare industry (including government). It also establishes a mechanism to provide needed training to assist organizations adopt common practices that are based on developed standards, regulatory requirements and appropriate practices. This represents a positive move towards needed standards to support expanded electronic health information exchange and to remove current barriers to that exchange. Care needs to be taken during the implementation process to obtain industry and government buy-in as well as identify needed funding sources to maintain an on-going technical assistance and education program.. Some of the noted milestones have been met or will be met soon. Full success, though, hinges on appropriate funding levels.

1.5.1 Lack of funding for start-up and on-going activities.

1.5.2 Difficulty in obtaining full government/industry buy-in (answering the "what's in it for me").

1.5.3 Difficulty in dispelling potentially long standing myths and/or cultural biases.

1.5.4 Lack of sufficient staffing support to implement and sustain any developed solution, educational program, web material, etc.

1.5.5 Difficulties in rolling out a comprehensive education program across a state with significant rural areas.

1.5.6 Lack of consistent technical security and privacy standards across applications.

1.5.7 Potential cost to the industry to adopt standards that may not be supported by existing technical infrastructure (and in some cases where the technical infrastructure does not exist).

1.6. OVERALL FEASIBILITY CONSIDERATIONS: Assuming the most significant barriers listed above can be effectively managed; successful implementation of the major activities described in this implementation plan is feasible. Feasibility will be impacted by the degree of industry and government involvement, government and industry buy-in and availability of funding and appropriately trained staff to support development, rollout and on-going maintenance.

1.7. IMPLICATION FOR IMPLEMENTATION EFFORTS BEYOND STATE BOUNDARIES

MULTI-STATE IMPLEMENTATION PLANS

To be developed – Oregon is partnering with other states in the region to develop, where feasible, regional standards and educational material. At this point, discussions are in the beginning phases.

NATIONAL-LEVEL RECOMMENDATIONS

HHS (specifically OCR and CMS) need to provide technical assistance and guidance to assist with the development of common sets of educational material that can be used as the basis for developing more nationally based education and standards adoption. Also, technical grants are needed to assist in developing common standards. HITSP can provide assistance with the development of technical standards but output from this project needs to go beyond mere recommendations.

1.6. NEXT STEPS This Implementation Plan reflects the contribution and feedback from willing participants from the Oregon HISPC Solutions and Implementation Working Group, Legal Working Group, the Oregon Medical Association, the Forum, OAHHS the Oregon Department of Human Services, the HISPC Steering Committee and others. The feedback process will continue following completion of the HISPC project to continually refine the plan and solicit needed involvement.

Efforts will continue to engage stakeholders as implementation of this solution moves forward. Broad involvement is required to achieve success. Concerns still exist regarding funding the implementation of this solution as well as other proposed Oregon solutions. The challenge of perpetuating the process and identifying needed funding sources is currently underway and will continue into the future.

Provider Authorization and Authentication Implementation Plan

1.1. PLAN TITLE: Implementation of Provider Authorization and Authentication

1.2. PLAN SUMMARY

1.2.1 BRIEF DESCRIPTION. This effort will focus on implementation of administrative and technical standards related to appropriate access authorization and authentication of providers, addressing authentication in a technical and non-technical environment.

1.2.2 **NEED A COORDINATED APPROACH TO IDENTIFYING, AUTHENTICATING AND AUTHORIZING PROVIDERS**. One of the more significant issues that was raised by the provider community was the need for a standard method of identifying and authenticating providers. The current lack of appropriate or trusted authentication creates significant trust issues. Providers are reluctant to share patient information with other providers given the difficulty in the lack of workable methods of authentication. The concern regarding liability and risk associated with inappropriate release to an individual or entity because a trusted method of authentication does not exist has resulted in needed health care information not being shared or not being shared in a timely manner.

Also, as the healthcare industry in Oregon moves more and more towards an electronic environment, a mechanism or organization to manage access (in essence authorization) is needed. That mechanism or organization needs to be neutral, trusted and must follow appropriate access management practices that allow appropriate access to health information as needed and prevent access to health information by unauthorized individuals or entities.

Access control and authentication mechanisms need to be standardized, follow appropriate security practices and comply with the requirements of the HIPAA security rule. It is likely health information exchanges or RHIOs will be collaborative organizations or established third party entities that are business associates of all participating covered entities. In either case, it is important to adhere to regulatory requirements and the statutory requirements of the likely to be enacted medical identity/identify theft legislation in Oregon.

1.2.2.1.	Engage the Oregon Medical Association (OMA), the Oregon Association of Hospitals and Health Systems (OAHHS), Oregon Health Sciences University (OHSU) and Oregon licensing boards in the design of a database that authenticates providers based on licensure credentials.
1.2.2.2.	Develop a standard approach to provider authentication and authorization that uses appropriate and feasible administrative and technical safeguards.
1.2.2.3.	Engage vendor partners as appropriate.

1.2.2.4.	Participate in national discussion as standards related to access control, authorization and authentication evolve.
1.2.2.5.	Collaborate with private and public sector partners to document and implement standard and appropriate access control, authorization and authentication standards that are scalable, address electronic and non-electronic data exchange and standardized across all existing and planned RHIOs/health information exchanges.
1.2.2.6	Designate a neutral third party or board to manage access control and authorization of providers, business associates and other individuals or entities with a valid reason to access patient or health plan member health information (also responsible for monitoring and assisting with the implementation of improvements and publication of new standards for access control, authorization and authentication).
1.2.2.7	Develop and implement an educational program to assist organizations in understanding standard access control, authorization and authentication (technical and administrative safeguards).
1.2.2.8	Develop a technical assistance program to assist in implementing administrative and technical components of access control, authorization and authentication. This includes assisting the industry in funding deployment where necessary

1.2.3 LEAD ORGANIZATION. The lead coordinating organization for this implementation plan is a currently being formed public and private sector consortia. The consortia will be responsible for development of standards related to access control, authorization and authentication. The Consortia will also assist with education and deployment (electronic and non-electronic, technical and administrative) of appropriate access control, authorization and authentication standards for organization level activity, inter-organizational data exchange and movement towards HIE standards for existing and planned RHIOs/HIE networks.

1**.2.4 KEY STAKEHOLDERS AFFECTED**. The following organizations, groups of stakeholders and interested parties will be affected by and/or primarily involved in various aspects of the implementation plan.

1.2.4.1. **Private Sector and State Partnership:** Oregon state government and private industry play an important part in developing a much needed partnership that assists with the development and implementation of electronic/non-electronic, technical and administrative standard access

control, authorization and authentication that works in today's mixed paper/electronic environment and into the future as HIE activity expands. Also, this partnership is important in assisting the public and private sector in implementing and assisting with funding identification to assist in successful deployment of standardized and trusted access control, authorization and authentication.

1.2.4.2 **Vendors:** The involvement of vendors is essential in developing the technical standards that assist in consistent and interoperable solutions to access control, authorization and authentication. Currently a variety of approaches are used and many are not interoperable. in the process as possible.

1.3. SCOPE: The scope of this plan includes formal adoption of appropriate access control mechanisms; individual or entity authorization to access the minimum amount of data necessary to perform required tasks related to quality healthcare, healthcare administrative activities, etc.; and deployment of appropriate authentication mechanisms that are appropriate to the type of data being exchanged or accessed. The project also includes needed education, vendor involvement to develop interoperable standards and assistance with deployment of standards governing appropriate access to identifiable patient or health plan member health information. This includes developing and implementing solutions that work in the current environment and assist with implementation of appropriate interoperable standards and mechanisms governing access control, authorization and authentication (administrative and technical). The scope of this implementation plan includes:

1.3.1 Engage the Oregon Medical Association (OMA), the Oregon Association of Hospitals and Health Systems (OAHHS), Oregon Health Sciences University (OHSU) and Oregon licensing boards in the design of a database that authenticates providers based on licensure credentials

1.3.2 Phase in levels of authentication and authorization beginning with provider to provider only authentication (e.g., leaving the decision regarding the exchange of individually identifiable health information (IIHI) to the provider and beginning with a tool to allow providers to validate that the requesting party is who they say they are and have appropriate credentials to use any exchanged IIHI appropriately)

1.3.3 Facilitate industry/government discussions regarding the development of access control, authorization and authentication standards (electronic and non-electronic, administrative and technical)

1.3.4 Designate a neutral third party to assist with initial implementation and continue to act as the access control, authorization, authentication technical assistance and oversight body as electronic initiatives move forward (at this point, the goal of the neutral third party will be focused on exchanges between organizations and not internal organizational implementation of appropriate access control, authorization and authentication mechanisms)

1.3.5 Develop and publish standards for access control, authorization and

authentication supported by the public and private sectors

1.3.6 Engage vendors to assist in development of technical supports needed to implement developed standards such that solutions will be interoperable and will work in today's environment and as Oregon moves towards broader use of HIEs/RHIOs

1.3.7 Implement endorsed appropriate practices (electronic and non-electronic, administrative and technical)

1.3.8 Educate and provide technical assistance with the implementation of appropriate access control, authorization and authentication standards.

1.3.9 Assist in seeking funding to assist especially small providers and RHIOs/HIEs in the development phase adopt standards and acquire needed technical supports

1.3.10 Explore the use of multi-factor authentication where necessary to additionally protect sensitive patient or health plan member health information

1.3.11 Monitor national activity and assist the public and private sector deploy new standards as they are finalized through the HITSP and other projects

1.4. TASKS, TIMELINE AND KEY MILESTONES: The major activities and tasks required to implement Provider Authorization and Authentication are currently being identified and are not available at this time to include in the implementation plan.

A summary of the Technical Assistance and Sharing Appropriate Practices deliverables in order of their estimated date of completion is included in Table 1:

Table 1. Deliverables: Implementation of Provider Authorization and Authentication for Oregon HIE

PROJECT PLAN REFERENCE	MILESTONES/DELIVERABLES	ESTIMATED COMPLETION DATE
1.3.1	Engage the Oregon Medical Association (OMA), the Oregon Association of Hospitals and Health Systems (OAHHS), Oregon Health Sciences University (OHSU) and Oregon licensing boards in the design of a database that authenticates providers based on licensure credentials.	10/1/07
1.3.2	Develop a standard approach to provider authentication and authorization that uses appropriate and feasible administrative and technical safeguards.	3/1/08
1.3.3	Engage vendor partners as appropriate.	7/1/07
1.3.4	Participate in national discussion as standards related to access control, authorization and authentication evolve.	On-going
1.3.5	Collaborate with private and public sector partners to document and implement standard	7/1/08

	and appropriate access control, authorization and authentication standards that are scalable, address electronic and non-electronic data exchange and standardized across all existing and planned RHIOs/health information exchanges.	
1.3.6	Designate a neutral third party or board to manage access control and authorization of providers, business associates and other individuals or entities with a valid reason to access patient or health plan member health information (also responsible for monitoring and assisting with the implementation of improvements and publication of new standards for access control, authorization and authentication).	7/1/08
1.3.7	Develop and implement an educational program to assist organizations in understanding standard access control, authorization and authentication (technical and administrative safeguards).	10/1/08
1.3.8	Develop a technical assistance program to assist in implementing administrative and technical components of access control, authorization and authentication. This includes assisting the industry in funding deployment where necessary	1/1/09

The first milestone, 1.3.1, addresses a project that was kicked off in March 2007. The project entails creating a database that includes provider credentials, provider contact information and related information to assist providers in validating or authenticating that a provider requesting patient health information is a valid entity or individual. The database also provides sufficient information to authenticate the provider making the request ensuring that he/she has sufficient credentials to appropriately use any patient health information provided.

The project has been funded by the Oregon Medical Association. Partnership with other major healthcare associations, providers and health plans (including the State of Oregon) has been successful and partner organizations have indicated a significant interest in participating in the development and population of the database. This serves two important needs of Oregon providers and health plans; it provides national provider identifier information and it provides a method of authenticating providers prior to forwarding any patient health information.

The database will include privacy and security safeguards that represent industry appropriate practice and adhere to the HIPAA privacy and security rules. In future phases

it can also be used as a front end authentication engine for RHIOs/HIEs across the state at the point in time such collaboratives are in a position to share patient health information electronically. In a future phase, access authentication will move from single factor (password) authentication to multi-factor authentication (password and digital certificate).

Phase one will include implementation of an NPI repository, sufficient information to authenticate the provider and a mechanism to require providers included in the database to update their information at least annually. The second phase will include the addition of quarterly data feeds from Oregon licensing boards to reasonably ensure data is current and the provider continues to be licensed to provide healthcare in Oregon. It is important to note that the database will not only include physicians, it will include all providers in the state of Oregon.

The database will be loaded with data provided by large providers, health plans and Oregon Medicaid. This means when the database is completed and available for use, a significant amount of data and the majority of providers in Oregon will be included in the database. Also, a process to authenticate and add small providers will be included to allow small providers, especially in rural areas, to enter their information in the database. There will be a charge to access the database but the cost will be minimal to only cover database administration (likely less than $20 per year per provider).

This represents an example of current activity underway in Oregon to address barriers identified as part of the Oregon HISPIC project. It also is a project where funding is not an issue. The Oregon Medical Association has committed to providing the development funding needed for this project.

1.5. POSSIBLE BARRIERS: This implementation plan addresses the essential need for the adoption of standard access management, authorization and authentication that will assist the industry today in addressing trust issues between organizations, improve the flow of electronic and non-electronic health information as needed in a timely manner and set the stage for adoption of standards that will assist in effectively managing access to IIHI for healthcare purposes and guard against inappropriate access to IIHI. This implementation plan includes the involvement of public sector, private sector and vendor partners to obtain buy-in and assist in implementing workable information access standards (technical and administrative). Without a widely adopted, interoperable solution, it will be difficult to address existing trust issues and deploy appropriate administrative and technical practices that will work in the current environment and as organizations move more and more towards formally established RHIOs/HIEs. Care needs to be taken during the implementation process to obtain industry, government and vendor buy-in as well as identify needed funding sources to develop standards, implement those standards along with potentially missing technical infrastructure, maintain on-going technical assistance and education program and provide for a neutral third party to assist in managing access across the state to IIHI.. Some of the noted milestones will be met soon. Full success, though, hinges on appropriate funding levels.

1.5.1 Lack of funding for start-up and on-going activities.

1.5.2 Difficulty in obtaining full government/industry buy-in (answering the “what’s in it for me”).

1.5.3 Difficulty in surmounting the existing longstanding trust issue.

1.5.4 Lack of sufficient staffing support to implement and sustain any developed solution, educational program, web material, etc.

1.5.5 Difficulty in creating an interoperable solution supported by needed vendors.

1.5.6 Lack of consistent technical and administrative access control, authorization and authentication standards across the industry and between vendor applications.

1.5.7 Potential cost to the industry to adopt standards that may not be supported by existing technical infrastructure (and in some cases where the technical infrastructure does not exist).

1.6. OVERALL FEASIBILITY CONSIDERATIONS: Assuming the most significant barriers listed above can be effectively managed, successful implementation of the major activities described in this implementation plan is feasible. Feasibility will be impacted by the degree of industry and government involvement, government and industry buy-in and availability of funding and appropriately trained staff to support development, rollout and on-going maintenance. Funding, once again, is probably the most significant barrier.

1.7. IMPLICATION FOR IMPLEMENTATION EFFORTS BEYOND STATE BOUNDRIES

MULTI-STATE IMPLEMENTATION PLANS

To be developed – Oregon is partnering with other states in the region to develop, where feasible, regional standards and educational material. At this point, discussions are in the beginning phases.

NATIONAL-LEVEL RECOMMENDATIONS

HHS (specifically CMS) need to provide technical assistance and guidance to assist with the deployment of standardized access control, authorization and authentication practices. Recently CMS published guidance regarding remote access. Key to that and not fully addressed are the required activities related to access control, authorization and authentication. Transmission of IIHI will be moving more and more towards electronic exchanges of data and the same concerns CMS raised regarding remote access apply to the sharing of data between organizations and through the deployment of an HIE. HITSP can provide assistance with the development of technical access control, authorization and authentication standards but output from this project needs to go beyond mere recommendations.

1.6. NEXT STEPS

The next steps involve the creation of the secure database. Once in place the database will be tested for functionality and loaded with provider information. Although support among providers is widespread, the database will need to be marketed to providers and health plans in Oregon to promote use. The database is planned to be ready for use by Fall of 2007. Additional enhancements are planned for the database, but a timeline has not yet been set for implementation.