Privacy and Security Solutions for Interoperable Health Information Exchange

Oregon's Final Assessment of Variation and Analysis of Solutions Report

Subcontract No.
RTI Project No. 9825

Prepared by:

Summer Boslaugh, Jody Pettit, Nancy Clarke, Chris Apgar
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

March 30, 2007

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 of Oregon Health Policy and Research

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

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

Nancy Clarke, Executive Director
Oregon Health Care Quality Corporation

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

Chris Apgar, CISSP President
Apgar and Associates, LLC

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

Bonnie Sailer, Project Assistant
Oregon Health Care Quality Corporation

&

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

Table of Contents

Executive Summary

The electronic exchange of health information holds the potential to revolutionize health care in many ways including through improved quality, cost efficiencies, enhanced patient/consumer engagement, and greater continuity of care. Within the broad arena of health information exchange (HIE) the Oregon Health Information Security and Privacy Collaboration (HISPC) is exploring the issues of privacy and security. Governor Ted Kulongoski appointed a HISPC Steering Committee with a breadth of expertise and depth of commitment to accomplish the work of the project. The project is a collaboration of the Oregon Health Care Quality Corporation and the Office for Oregon Health Policy and Research.

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.

Values

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

Critical Issues

The health care environment is changing: electronic health records are replacing paper records and health information is increasingly being exchanged electronically. The electronic exchange of information has the potential to revolutionize health care in many ways including through improved quality, cost efficiencies, enhanced patient/consumer engagement, and greater continuity of care. While the technology to do this is emerging, there is still a great deal of work to be done to allow for a smooth transition into this new world.

To function in this new environment, trust relationships must be built between individuals and organizations involved in health care or the handling of health information. Multiple high-profile inappropriate disclosures have heightened consumer concern for the privacy and security of their electronic health information. The need to protect individuals' privacy must be balanced with the need to share individuals' health information so that care is safe, effective and efficient. Achievement of this balance between potentially conflicting values necessitates an approach that includes an enhanced role for the individual in determining the flow of their health information.

Recommended Solutions

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 provider*s*

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

11. **State Leadership**
    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 identified solutions.

1. Background and Purpose

1.1 Description of the purpose and scope of this report

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.

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.

In this phase of the project, 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 advocacy organizations participated in this phase. The purpose of this report is to present the findings.

1.2 Level of HIT Development in Oregon

Oregon is a state where there exist vast differences in the sophistication and level of health information technology. There are several highly developed communication networks that exist to address technical changes, exchange of information, privacy issues and security issues. These networks include both urban and rural communities and organizations located in those communities. They do not necessarily represent what would be an interoperable network between communities.

On the other hand, there are still a fair number of healthcare organizations that have yet to engage in longstanding statewide discussions regarding appropriate use of technology to exchange electronic health information and often not even adhering to appropriate privacy and security standards. Attempts have been made to engage these stakeholders but success has been somewhat limited. It is important to note, though, this is not just an Oregon phenomena but a national one.

Oregon does have the advantage of long term partnerships between the broad spectrum of healthcare stakeholders. The level of collaboration in Oregon is high and relatively amicable. It has led to the establishment of industry standards ranging from privacy to security to electronic health information exchange. There is a high degree of interest within the state to develop mutually acceptable practices and solutions to improve health information exchange and advance the use of technology for health information exchange, higher quality healthcare, increased efficiencies, etc. Advances in HIE are seen not as merely building an individual organizational competitive advantage but an overall increase in healthcare quality and efficiency and a way to better serve Oregonians relying on the Oregon healthcare system.

Communication Strategies & Participants

Oregon is home to a number of associations that have demonstrated their effectiveness in pulling member organizations together, partnering with each other and enhancing communication related to the development of HIE standards as well as inter-organizational communication. One of the core organizations that has been effective in bringing multiple stakeholders to the table is the Oregon and SW Washington Healthcare, Privacy and Security Forum (the Forum). The Forum was established in May 2000 initially to assist the Oregon healthcare industry with HIPAA implementation issues. Since then, the Forum has expanded its focus to address the broader issues of HIE facing the industry and to continue to work collaboratively to develop standards that enhance and expand HIE.

Forum membership includes the Oregon Association of Hospitals and Health Systems (OAHHS), the Oregon Medical Association (OMA), the Oregon Dental Association (ODA), the Oregon Board of Medical Examiners, the Oregon Department of Human Resources (Medicaid agency, state mental health administration, long term care oversight, public health, etc.), health plans, providers, vendors and clearinghouses. The Forum is a Workgroup for Electronic Data Interchange (WEDI) Regional Affiliate actively tying what is occurring at a national level with efforts to improve HIE in Oregon. The Forum has the advantage of acting as a neutral organization that encourages and supports on-going communication between stakeholders and improve HIE. However, one disadvantage of the existing Forum structure is it does not generally involve consumers but this is being considered at this time.

In addition to the activities of the Forum, the OAHHS, the OMA, the ODA and others continue to work with member organizations to advance HIE, provide needed education and strive to engage member organizations in HIE discussions as well as implement appropriate privacy and security standards which often is one of the more significant barriers to information exchange between especially providers.

Several communities, rural and urban, are making significant progress in planning for the implementation of a community health record. Some of these communities have participated in the Oregon HISPC project with the intent of addressing existing business practice and legal barriers and developing standards for the deployment of a community health record. The general consensus of the industry is it would be beneficial to, where feasible, establish a standard HIE model which would improve interoperability between organizations and, where deployed, community health records.

Summary

Oregon is moving forward with initiatives to improve HIE within the state and the region. Well established groups have been working within the industry for a number of years and have developed collaborative partnerships that assist in achieving success in standards development, improved quality of care and more efficient healthcare operations. This strong web of mutually beneficial partnerships includes associations, government, large and small organizations, cross-state collaborative, and others with a tie to national discussions related to HIE improvement. Oregon has made significant progress but realizes that additional participation is needed. Efforts to involve smaller providers needs to expand, additional education is needed and consumers need to be more actively involved as HIE expands and consumer health information proliferates.

1.3 Description of Report Limitations

Following is a summary of the Oregon HISPC Project interim solutions report limitations. Many of the listed report limitations will likely be addressed in the final solutions report.

1. Broad Stakeholder Involvement: The solutions work group attempted to reach out to stakeholders from across the state but were not as successful as the project team would have desired in engaging rural stakeholders. The project team traveled to several communities throughout the state to better engage these stakeholders. However, more extensive involvement of stakeholders throughout the state is needed.

2. Consumer Involvement: Consumers and consumer groups have been invited to participate in the work group but in spite of multiple efforts at outreach, few have become actively involved in the project. The project team continues to reach out to consumer groups through e-mail, open meetings, etc. It is hoped that when the final solutions and implementation report is drafted, it will reflect more consumer input than the interim report.
3. Time and Resource Limitations: Time and resource constraints limited the depth and breadth of feedback we were able to gather as we explored proposed solutions, reviewed how proposed solutions would address identified barriers and obtained buy-in from involved stakeholder groups. The project team will continue to work with stakeholder groups to fully explore proposed solutions, viability of solutions and stakeholder support. This is reflected in this final report.
4. Political Support: Political support is needed to implement identified solutions which include possible needed legislative action, fiscal support, etc. At this point, we have not successfully fully engaged legislators and other critical government leaders.
5. Regional Collaboration: One of the significant barriers noted was related to inter-state communication of health information due to differences in state law. There was not sufficient time to analyze these barriers and collaborate with sister states in an effort to develop regional solutions that address barriers to inter-state data exchange. It should be noted, though, that Oregon and Washington have formed a strong collaborative that will hopefully assist in addressing outstanding inter-state issues in the Northwest.

2. Assessment of Variation

2.1 Methodology Section

Under the guidance of the Oregon HISPC Steering Committee appointed by the Governor, project staff convened two groups of privacy and security experts from throughout the state to form the Variations Work Group (VWG) and the Legal Work Group (LWG). The project team sought to engage a diverse group of experts representing key stakeholder groups and a variety of care delivery settings. The members represented hospitals, physician groups, health plans, public health agencies, community clinics, pharmacies, corrections facilities, state government, healthcare associations and other organizations involved in the exchange of health information.

Variations Work Group

Potential VWG members were identified by project staff, Steering Committee members and other key leaders from around the state. Although the VWG was originally envisioned as a small group with set membership, it quickly became clear that in order to address the wide array of issues brought up in the HIE scenarios, a larger and more dynamic group was preferable. In order to accomplish this we again sought the suggestions of our partners. Work group members included privacy officers, security officers, quality staff, medical records managers, healthcare attorneys, vendors and others from a variety of organizations involved in health information exchange.

We convened four VWG meetings during the month of August 2006. Many individuals attended more than one of these meetings, but there were also new participants present at each one. In addition to the scheduled work group meetings, individual and small group meetings were held with the goal of filling in representation missing in the larger group. A meeting of state level public health experts was convened to address the public health scenarios and mental health experts were also consulted and provided some business practices for the scenarios involving mental health.

During each meeting participants discussed four or five scenarios, emphasizing the business practices followed by their organization or other organizations they are familiar with. The meetings were facilitated by Nancy Clarke, Executive Director of the Oregon Health Care Quality Corporation, who successfully directed participants to discuss the unique privacy and security issues raised in each scenario. For each scenario discussion, the scenario was presented to the group and then possible privacy and security issues and concerns were highlighted to guide the group's discussion. Members were asked to describe general business processes they were aware of in their organization or others in the state. Discussion of other issues and concerns related to privacy and security (but not specifically presented in the scenarios) also occurred.

Legal Work Group (LWG)

The LWG consisted of experts from key legal stakeholder groups in the state including representatives of hospitals, consumers, health plans, health systems, associations and public health agencies. The LWG assisted in evaluating potential security and privacy legal barriers to HIE through focused discussions. In addition, a subgroup of the VWG and LWG convened to identify the legal drivers underlying identified business practice.

Stakeholder Involvement

Once the business practices had been identified for each scenario Oregon HISPC staff compiled them into a document to share with the work group members and stakeholders. We used the online tool Survey Monkey to disseminate identified business practices in an easy-to-digest format with interactive options for readers to contribute additional business practices. Although we did not receive many responses, the tool enabled us to inform over 300 stakeholders about the status of the project.

Synthesis of Business Practices

We engaged the VWG and Steering Committee members in a number of one-on-one and small group meetings to help synthesize the 150+ business practices identified. These groups discussed the common challenges illustrated by documented business practices. The goal of this process was to distill the long list of practices to a group if key issues the Steering Committee could evaluate and prioritize for the Solutions Work Group.

2.2 Summary of relevant findings for information exchange

The following is a summary of critical observations and key issues discussed in the report and overall issues raised by the VWG, Steering Committee, and project staff.

Accessing Information

Patient identification
In an electronic environment providers, business associates and health plans may have access to many patient health records, allowing for the sharing of the most timely health information to improve health outcomes and more efficient administrative activities such as payment. Access to a large repository of information may increase the likelihood of duplicate names requiring the provider, health plan or business associate to access multiple records to identify which is the correct one. How can correct patient identification be ensured without inappropriate disclosures?

Authentication, authorization and access control
To protect the privacy and security of health information it is necessary to ensure that only the appropriate people have access to only the appropriate information (HIPAA and Oregon law minimum necessary requirements). The complexity of this task is magnified in a health information exchange network. In such a network, it is necessary (1) to authenticate a person or entity who desires access is who he or she (or the entity) claims to be, (2) to establish that the person or entity has the authority to access the network, and (3) to limit his or her (or entity) access using role-based controls while not hindering provisions of quality and timely healthcare (such as in treatment situations where the minimum necessary standard does not apply). How would an authentication and access system work in Oregon? How do we apply the concepts of role-based access in an environment of health information exchange? Does existing technology support appropriate access control, authorization and authentication control mechanisms (including appropriate audit tracking)?

Circle of care
With greater flow of information in an electronic environment, patients will experience improved coordination of care. Protections must be in place to ensure that only those providers and potentially health plans or business associates within the circle of care can access personal health information. How should circle of care be defined? How should circle of care access be kept up-to-date so that only providers or other entities currently involved in the patient's care have access to patient's health information? What are the implications of "push" information sharing, when providers are automatically notified of information (e.g. lab results forwarding), versus "pull" information sharing, when providers must request information? Does the circle of care need to address the involvement of other than providers in patient health care support (such as case managers, family, community supports, etc.)?

Patient use
Electronic health records offer the opportunity for patients to have greater access to their health information and take a more active role in managing their own health. Should patients be able to see any or all of their health records? Are there any risks of giving patients too much access to their health records? How can we assist patients access and understand their health records? How can we assure established access processes works for patients of all backgrounds and abilities? How would patient authorization and authentication work?

Proper use
Health information exchange increases the ease with which information can flow within an organization and between organizations. This allows for better coordination of care, greater efficiency in administrative processes and likely improves the quality of care but also an increase in the number of potential viewers of the information. How can patients be sure that only appropriate people see their records and that viewer sees only the minimum necessary information? How does this apply to treatment where, with few exceptions (specially sensitive information), the minimum necessary standard does not need to be adhered to under HPAA and Oregon law?

Using Information

Specially protected information
Oregon and other federal laws about specially protected health information (i.e. related to minors, substance abuse, mental health, HIV status, sexually transmitted diseases and genetic information) create a secondary layer of caution beyond HIPAA for sharing sensitive information. Oregon's providers vary widely in their interpretation of when and how to share specially protected information and what is required before such information may be shared. Are the laws and protections as written suitable and sufficient in an electronic environment? How can we reduce variation in the ways these laws are applied? Should all health information be protected equally?

Redacting
In an electronic environment the ability to redact specially protected information from a health record is more complicated than in a paper world. How will personal health information be protected from improper sharing when health records are sent electronically? How will this work in an HIE/RHIO environment.

Secondary use
Electronic health records have the potential to provide public good by facilitating access to health information for the purposes of public health reporting, bioterrorism event monitoring, disaster preparedness, health care quality improvement support, and appropriately constructed research. What kind of information should be shared for non-treatment, payment or healthcare operations purposes (secondary use of data)? How should this sort of use be authorized and managed?

Patient Involvement
Many patients are not fully aware of how their health information is used and who has access to it. With increased exchange of large quantities of health information in an electronic environment, patients' sensitivities to inappropriate disclosures are greatly heightened. Is there a more effective way of educating and engaging patients than distribution of the Notice of Privacy Practices? What is the patients' role in managing their inclusion in community-wide health information networks? How should patients be empowered to allow or restrict access by users to all or part of their information? Should there be exceptions to what they can restrict access to (i.e. scheduled drugs)? How will such restrictions, if established, impact care such as in emergent situations?

Protecting Information

Assuring an accurate, current record
Health status and treatment plans are constantly changing. Information about a patient's health may come from a variety of sources. How can we take advantage of the capabilities of electronic health information exchange to ensure that health records are up-to-date and accurate? How should we define what is relevant and important to a health record? How can we ensure that if amendments or updates are made to the health record, these changes are reflected in all copies of the record? Should the health record include other related information such as case management reports, community care supports, etc.?

Data transmission security
Electronic health information exchange will allow providers, health plans and business associates to send and review health information more easily, both internally and externally. If effectively implemented,

patients changing doctors or seeing specialists will no longer experience delayed care while waiting for records to be sent. What minimum standards need to be developed to ensure the technical security of electronic transmissions of health information? How can such standards be enforced? How do we assure all of Oregon's providers, health plans and business associates can appropriately participate regardless of their level of IT implementation?

Tracking Access/Audit Trails
As health information is increasingly available electronically, it is important to do as much as possible to prevent the information from being inappropriately accessed or shared. However, in the event a breach of security occurs, it is essential to have a robust system of audit trails to track access to a patient's record so that appropriate steps can be taken to reasonably ensure appropriate mitigation, appropriate application of sanctions and that inappropriate access is detected and does not reoccur. In addition to appropriate audit trails, appropriate privacy/security protections require the establishment of a well trained security/privacy incident response team at the organization level and at the RHIO/HIE level. What standards surrounding maintaining audit trails are needed? How can we learn from mistakes and continually improve the security protections of health information? What are the standards for formation and oversight of security/privacy incident response teams (organization level and RHIO/HIE level)? How are sanctions implemented and who is responsible for application of sanctions?

Accountability Concerns

Increased liability
Improved health information exchange may result in large quantities of patient health information being sent to providers, health plans and business associates without an immediate tie to a visit for treatment, payment and healthcare operations. Will increased provider, health plan and business associate liability result from the creation of more information than can be reasonably used? Will healthcare organizations also experience greater liability? How should we address issues that arise from having too much information?

Need for effective sanctions
In order to rebuild public trust in healthcare organizations' ability to appropriately protect identifiable personal health information, a universal standard needs to be applied for individuals and entities that violate the privacy and security requirements regarding the use and exchange of electronic health information. How can this be improved? What are other ways to ensure the public trust? Despite all safeguards to protect security and privacy of health information, inappropriate disclosures will inevitably occur. What should happen when inappropriate disclosure occurs? Who is responsible (organization level and RHIO/HIE level)?

Medical Identity theft
Increased flow of electronic health information could potentially create greater opportunity for medical identity theft. How can patients be reasonably assured healthcare organizations and partnerships such as RHIOs protect their health information from this threat?

2.3 Treatment (Scenarios 1–4)

2.3.a. Stakeholders

The key contributors in defining the business practices based on the scenarios dealing with treatment were Hospitals and Physician Groups.

2.3.b. Domains

Information use and disclosure policy (domain 9), specifically the release of specially protected information, was a very important domain in the discussion of the four treatment scenarios. Oregon laws about specially protected health information (i.e. related to minors, substance abuse, mental health, HIV status, sexually transmitted diseases and genetic information) create a secondary layer of caution beyond HIPAA for sharing sensitive information.

Oregon's providers vary widely in their interpretation of when and how to share specially protected information and authorization required. This is evidenced in the variation of business practice. In the case of mental health information as presented in Patient Care Scenario A, some hospitals will segregate the information from the rest of the health record while others do not. We found similar variation with regard to substance abuse treatment in Patient Care Scenario B. This variation may in part be caused by different interpretations of ORS 179.505 and 430.399 and 42 CFR pt. 2, which govern release of some types of sensitive information. Discussions of the VWG revealed a good deal of confusion about legal restrictions and exchange requirements.

The following domains were also relevant to the business practices discussed:

1) User and entity authentication
2) Information authorization and access controls
3) Patient and provider identification
4) Information transmission security or exchange protocols
7) Administrative or physical security safeguards
8) State law restrictions

2.3.c. Critical Observations

Providers often go straight to other providers to obtain information they feel is necessary for treatment. As one Variation Work Group participant stated, "If the doctors need information to make a medical decision, then they need it. So they can usually get it from other doctors, who understand that." However, other hospital or medical office staff (and often providers themselves) encounter many situations where it is hard to define who falls within the circle of care and what information should be released. This is particularly difficult in situations involving specially protected information as in all the Patient Care Scenarios.

Another common issue was the difficulty all organizations involved in the Variations Work Group had in redacting specially protected information electronically. This obstacle limits electronic HIE between and within organizations. Organizations with an EHR generally print a copy of a medical record, use a black pen to mark out specially protected information and then fax the record to another provider. Much of this is associated with existing technical issues with the EHR that does not fully accommodate segregation of especially specially sensitive information.

Discussions surrounding these scenarios also revealed the issue of enforcement of privacy and security regulations. Organizations have varying policies in place to address the issue of enforcement. For many organizations, enforcement often relies on policies that impose audit trails to track violations and dictate actions taken to mitigate harm, rather than on policies that strengthen systems to reduce the likelihood of violations. In other words, a number of organizations have not fully implemented the HIPAA security rule.

Discussion of the Genetic Law in Oregon arose regarding Patient Care Scenario D. The law states that all patients must be given the option to opt out of having their coded or anonymous genetic information used for research. VWG members expressed confusion surrounding what qualifies as genetic information. Also, concern on the part of consumers about how the data will be used and confusion regarding what genetic data could be used for has resulted in a 70% opt out rate.

2.4 Payment (Scenario 5)

2.4.a. Stakeholders

The key contributors in identifying the business practices for the scenario dealing with payment were Hospitals, Physician Groups, Health Plans and Correctional Facilities.

2.4.b. Domains

The domain of information authorization and access controls (domain 2) was very relevant to the discussion of the payment scenario. To protect the privacy and security of health information, it is necessary to reasonably ensure that only appropriate people have access to the appropriate information. The complexity of this task is magnified in a health information exchange network. In such a network, it is necessary (1) to authenticate that a person or entity who desires access is who he or she (or entity) claims to be, (2) to establish that the person or entity has the authority to access the network, and (3) to limit his or her or entity access using role-based controls. Many VWG members expressed concern that current systems do not adequately enforce role-based access, both because of technological limitations and perceived complexity of the task.

The following domains were also relevant to the business practices discussed:

1) User and entity authentication
6) Information audits that record and monitor activity
7) Administrative or physical security safeguards
9) Information use and disclosure policy

2.4.c. Critical Observations

In addition to concerns about how to allow appropriate access to an EHR (see discussion in 2.2.2), this scenario also prompted an interesting discussion about health plans' desire to access providers' EHRs and health plan reluctance to learning different systems for each of the organizations they work with. Health plans want access to the information as needed for business operations, but they want the ease of a report processed and prepared by the provider. The difficulty of learning many systems diminishes when the health plan and facility are part of the same organization. This, though, is generally not the situation. Although in this situation, protections to enforce health plan access to only the minimum necessary information is critical. The group spent a lot of time discussing software capabilities to control access in a role-based fashion.

The issue of proactive and retroactive protection of information (see discussion of enforcement of protections in 2.1.3) is also important in this scenario. Variation exists concerning organizations' actions to diminish the opportunity for violations and sanctions for violations when they occur.

2.5 RHIO (Scenario 6)

2.5.a. Stakeholders

2.5.b. Domains

2.5.c. Critical Observations

This scenario posed greater difficulty for the VWG in defining existing business practices because it is still generally hypothetical in our state. Because Regional Health Information Organization (RHIO) efforts are still in the nascent stages in Oregon, organizations are currently in the process of developing practices or policies to guide interaction.

The scenario prompted a lively discussion about RHIOs in general and work group members raised a variety of concerns. Consensus was reached that the scope of any RHIO needs to be very specific and transparent. Concerns were raised about enacting certain requirements such as redacting and honoring genetic opt out requests. With a RHIO, authorization, authentication, audit and access control become even more important..

2.6 Research (Scenario 7)

2.6.a. Stakeholders

The key contributors to the business practices for the scenario dealing with research are Hospitals, Universities and Researchers.

2.6.b. Domains

Information authorization and access controls (domain 2), particularly as related to patient authorization, were important in the discussion of this scenario. All the work group members agreed that IRB approval and, where appropriate, patient authorization is needed to conduct research. Parental or guardian consent would be required for minors to continue to participate in IRB approved research.

The following domains were also relevant to the business practices discussed:

8) State law restrictions
9) Information use and disclosure policy

2.6.c. Critical Observations

Health information exchange increases the ease with which information can flow within an organization and between organizations. This allows for better coordination of care but also an increase in the number of potential viewers of the information. In the case of the Research Data Use Scenario, the investigator could potentially have access to the patient data even if he/she was denied an extension of the project.

Issues with Oregon's Genetic Opt Out law were raised again with this scenario. Members noted it may be difficult to apply the notification provision of the law to third parties in an electronic environment.

Electronic health records have the potential to provide public good by facilitating access to health information for the purposes of public health and quality research. The group discussed the kind of information that should be shared for non-treatment purposes.

2.7 Law Enforcement (Scenario 8)

2.7.a. Stakeholders

The key contributors to the business practices for the scenario dealing with law enforcement are Hospitals and State Government.

2.7.b. Domains

State law restrictions (domain 8), specifically ORS 676.260, and information authorization and access controls (domain 2) were both highly relevant to this scenario. In Oregon, emergency room staff must report an elevated blood alcohol level to law enforcement if the patient was a driver in a traffic accident and a blood alcohol level test was performed. In all other cases the hospital needs patient authorization or a warrant for arrest to release blood alcohol level to law enforcement.

The following domains were also relevant to the business practices discussed:

8) State law restrictions
9) Information use and disclosure policy

2.7.c. Critical Observations

This scenario prompted a lot of discussion by members. A number of hospitals in the state have been working to educate law enforcement officers and ER staff about what specific patient information law enforcement can ask for in the ER. The hospitals developed a form for law enforcement use that specifies information they can request (without patient authorization) in order to identify or locate a suspect. In communities where hospitals have engaged law enforcement, relations between ER staff and law enforcement have greatly improved.

Several members of the group expressed concern about how personal health information would be protected in situations where ER staff and law enforcement officers have close personal (several group members knew of health care workers married to law enforcement officers) or professional relationships. The group speculated that information might flow more freely through informal channels in such situations.

2.8 Prescription Drug Use/Benefit (Scenarios 9 and 10)

2.8.a. Stakeholders

The key contributors to the business practices for the scenario dealing with prescription drug use/benefit are Hospitals, Physician Groups, Health Systems, State Government and Companies/Purchasers.

2.8.b. Domains

The following domains were relevant to the business practices discussed:

7) Administrative or physical security safeguards
8) State law restrictions
9) Information use and disclosure policy

2.8.c. Critical Observations

The issue of Pharmacy Benefit Managers prompted little discussion by the group. Everyone generally agreed that the PBM did not need access to the full EHR in the case of either scenario. Consensus was also reached in the discussion of Pharmacy Benefit Scenario B that PBM1 could complete a review of the companies' prescription drug use and associated costs by looking only at de-identified information.

2.9 Healthcare Operations/Marketing (Scenarios 11 and 12)

2.9.a. Stakeholders

The key contributors to the business practices for the scenario dealing with healthcare operations and marketing are Hospitals and Clinics.

2.9.b. Domains

The proper use aspect of the information use and disclosure policy domain (domain 9) was very relevant to the discussions about use of personal health information for marketing purposes. An EHR allows for easy transmission of personal health information for improved care, but also potentially for marketing purposes. The VWG identified multiple business practices with guidelines and authorization policies to govern the use of information and the notification of use.

The following domains were also relevant to the business practices discussed:

1) User and entity authentication
2) Information authorization and access controls
4) Information transmission security or exchange protocols
7) Administrative or physical security safeguards

2.9.c. Critical Observations

The two big issues that arose during the discussion of these scenarios were the question of what type of marketing directly to a targeted group of patients is permissible and how patient data is transferred within an organization. Consensus was generally reached that targeted contact of prior patients is allowed for education, fundraising and research purposes, but not for marketing (with limited exceptions allowed by the HIPAA privacy rule). However, it is often hard to differentiate between marketing and education about health care services. The VWG members from hospitals and physician groups had varying policies defining the difference between marketing and education.

While much of the discussion in the VWG meetings focused on how data is transferred from one organization to another, these two scenarios highlight the need for organizations to think about how data is transferred internally. VWG members described instances of extensive patient data being emailed to the marketing department without necessary security measures. Policies to ensure secure transfer are often much less stringently enforced.

2.10 Public Health/Bioterrorism (Scenario 13)

2.10.a. Stakeholders

The key contributors to the business practices for the scenario dealing with bioterrorism are Laboratories, Public Health Agencies and State Government.

2.10.b. Domains

Appropriate use of information and disclosure policy (domain 9) was extremely relevant to the bioterrorism scenario; specifically the use of personal health information outside basic treatment, payment and healthcare operations. Electronic health records can be used to provide public good by facilitating access to health information for the purposes of public health reporting, bioterrorism event monitoring, disaster preparedness, health care quality improvement support, and research. However, care must be taken to ensure that personal health information is shared appropriately in these situations, only to the necessary parties and, where feasible, as de-identified information.

State law restrictions (domain 8) were also relevant to the business practices discussed, as many of the guidelines followed by state and local public health departments are codified in state law (e.g. ORS 433, which deals in general with the actions of the state public health departments).

2.10.c. Critical Observations

Discussion of this scenario revealed frustration felt by state public health staff with law enforcement regarding the flow of information in an investigation. State public health employees feel that they provide all their data to law enforcement to facilitate an investigation, but are then cut out of the information loop and must rely on press releases for any additional data. There was also concern about whether law enforcement is subject to laws and regulations to protect the privacy and security of information that is shared with them, and if so, the specifics outlined in these laws and regulations.

2.11 Employee Health (Scenario 14)

2.11.a. Stakeholders

The key contributors to the business practices for the scenario dealing with employee health are Hospitals and Physician Groups.

2.11.b. Domains

Discussion of this scenario focused primarily on information authorization and access control (domain 2) on the part of the employer. To protect the privacy and security of health information it is necessary to ensure that only the appropriate people have access to only the appropriate information. None of the VWG members reported that an employer would have access to an EHR. Exchange of health information from provider to employer generally is handled by the patient on paper rather than electronically. The patient would receive paperwork from the provider and then deliver it to his/her employer. Also, any information requested by the employer on behalf of the patient requires a signed authorization by the patient.

The following domains were also relevant to the business practices discussed:

4) Information transmission security or exchange protocols
7) Administrative or physical security safeguards
9) Information use and disclosure policy

2.11.c. Critical Observations

One concern that arose was the case of a patient who works for a health care organization (e.g. at a health systems, health plan, etc). In this case it would be easier for the employer to gain access to the

patient's health record if he/she saw a provider who worked for the same health care organization. VWG members expressed concern that health care organizations may or may not have appropriate privacy and security protections in place to safeguard employee patient data.

2.12 Public Health (Scenarios 15–17)

2.12.a. Stakeholders

The key contributors to the business practices for the scenario dealing with public health are Laboratories, Physician Groups, Public Health Agencies, Community Clinics and Health Centers and Homeless Shelters.

2.12.b. Domains

Information transmission security (domain 4) is particularly relevant based on the business practices discussed in this scenario. Electronic health information exchange allows the state public health department to better track screenings and utilization of services. Like any other health organization, a high level of security is essential for the transmission of this data for public health purposes. The state public health department is currently working to update its exchange system and add new capabilities to better protect the privacy and security of information that is exchanged.

The following domains were also relevant to the business practices discussed:

2) Information authorization and access controls
7) Administrative or physical security safeguards
8) State law restrictions
9) Information use and disclosure policy

2.12.c. Critical Observations

When these scenarios were first discussed there were few public health people at the meeting. The group developed the most likely list of business practices based on their experience with public health situations. A subsequent meeting was held with a group of public health stakeholders who provided a very different list of business practices. A concern was raised that the lack of knowledge of public health practices by other health care stakeholders could indicate that patients are not informed by the medical community of public health consequences.

The VWG was particularly conflicted about the homeless shelter scenario. There was a great deal of discussion surrounding which organizations are covered entities and the proper way to interact with organizations that are not subject to HIPAA regulation.

2.13 State Government Oversight (Scenario 18)

2.13.a. Stakeholders

The key contributors to the business practices for the scenario dealing with state government oversight are Public Health Agencies and State Government.

2.13.b. Domains

As in the case of the bioterrorism scenario, much of the discussion of the government oversight scenario focused on information use and disclosure policy (domain 9). Employees of various state-run health agencies expressed that feeling that while oversight is doable at individual agencies, difficulties arise when blending data from different agencies because the information was collected with different intensions and permissions. In order to provide patient identifiable data for secondary public health use, health organizations need either patient authorization or a legal mandate.

The information authorization and access controls domain was also relevant to the business practices discussed.

2.13.c. Critical Observations

The greatest concern the VWG members had regarding this scenario is the confusion surrounding how one asserts, proves, or verifies that an organization is acting in a health oversight capacity.

3. Summary of Key Findings from the Assessment of Variations Report

The Assessment of Variations Report presented the 174 individual business practices generated by the VWG comprised of individuals from hospitals, physician groups, health plans, public health agencies, community clinics, pharmacies, corrections facilities, state government and other organizations involved in the exchange of health information. The business practices were described during discussions of the 18 scenarios provided by RTI detailing situations requiring the sharing of health information for the purpose of patient care; payment; RHIO; data use for research purposes; law enforcement; pharmacy benefits; health care operations; bioterrorism; employment; public health; health oversight.

3.1 Summary of Findings

The greatest barriers to health information exchange in Oregon are a set of universal challenges that all organizations participating in HISPC encounter. The following is a summary of those challenging issues discussed in the variations report and overall issues raised by the VWG, Steering Committee, and project staff.

Patient Involvement
With increasing exchange of health information in an electronic environment, patients have the opportunity for easier access to their health information, to better understand it and be involved in its uses. This electronic environment also results in heightened concerns about inappropriate disclosure. One of the most challenging issues is defining the patient role in accessing and directing the use of their health record.

- Patient access to record
  How can we help patients access, understand and assure the correctness of their health records? How can we assure this works for patients of all backgrounds and abilities? How much access should patients have to their health information? Should there be exceptions?

- Patient control of access by others
  What is the patient's role in determining his/her participation in community-wide health information networks? Will this role require changes in the Notice of Privacy Practices, require a new Notice of Privacy Practices or the way it is implemented?

Patient identification
In an electronic environment providers may have access to many patient health records, allowing the sharing of the most timely health information to improve health outcomes. Health plans may also have access to health information for many health plan members to assist with prompt payment of claims, pre-authorization of services, etc. Access to a large repository of information may also increase the likelihood of duplicate names requiring the provider, the health plan or business associate to look at multiple records to identify which is the correct one. How can correct patient identification be ensured without inappropriate disclosures?

Authentication, authorization and access control
To protect the privacy and security of health information it is necessary to ensure that only the appropriate people have access to only the appropriate information. The complexity of this task is magnified in a health information exchange network. In such a network, it is necessary (1) to authenticate that a person who desires access is who he or she claims to be, (2) to establish that the person has the authority to access the network (which requires establishment of a designated authority to grant access and authentication credentials), and (3) to limit his or her access using role-based controls. How would an authentication and access system work in Oregon? How do we apply the concepts of role-based access in an environment of health information exchange?

Circle of care
With improved access to information, patients may experience improved coordination of care. Protections must be in place to ensure that only those individuals involved in the patient's care can access personal health information. How should circle of care be defined? How should circle of care access be kept up-to-date so that only those individuals currently involved in the patient's care have access to patient's health information? What are the implications of "push" information sharing, when providers are automatically notified of information (e.g. lab results forwarding), versus "pull" information sharing, when providers must request information? If non-providers (e.g., case workers, family, etc.) are defined as part of the circle of care, how is access to needed health information accommodated?

Specially protected information
Oregon and federal laws about specially protected health information (i.e. related to minors, substance abuse, mental health, HIV status, sexually transmitted diseases and genetic information) create a secondary layer of caution (beyond HIPAA) for sharing sensitive information. Oregon's providers vary widely in their interpretation of when and how to share specially protected information. Are the laws and protections as written suitable and sufficient in an electronic environment? How can we reduce variation in the ways these laws are applied? Should all health information be protected equally? How can an electronic authorization for release be constructed and implemented?

Assuring an accurate, current record
Health status and treatment plans are constantly changing. Information about a patient's health may come from a variety of sources. How can we take advantage of the capabilities of electronic health information exchange to ensure that health records are up-to-date and accurate? How should we define what is relevant and important to a health record? How does a patient or legal representative amend or request an amendment to a record? How can we ensure that if amendments or updates are made to the health record, these changes are reflected in all copies of the record and distributed to individuals or entities who were previously provided a copy of the health record?

Medical identity theft
Increased flow of electronic health information could potentially create greater opportunity for identity theft, including medical identity theft. While the public has long been aware of the potential of financial identity theft, medical identity theft is only now beginning to receive attention. It occurs when someone uses a person's name and/or other parts of their identity – such as their insurance information – to obtain or make false claims for medical services or goods. How can patients be assured that healthcare organizations protect their health information from this threat? How can we ensure that health care organizations are responsive to the needs of medical identity theft victims? How are required practices to protect against medical identity theft enforced?

3.2 Effective Practices

See Appendices

3.3 Identified Variations Not Addressed

When the Steering Committee prioritized the key issues identified by the VWG, the following, while still considered important issues, were felt to be of lower priority, and therefore were not addressed in solutions work group meetings and are not addressed directly in the proposed solutions in the report. All of these issues are significant and it is recommended that they be revisited at a later time.

Proper use
Health information exchange increases the ease with which information can flow within an organization and between organizations. This allows for better efficiency and quality of care. However, it also increases the number of potential viewers of the information and the amount of information viewers can

access. How can patients be sure that only appropriate people can access their records? How can they be sure that viewers see only the minimum necessary information (which does not apply to treatment)?

Secondary use
Electronic health records have the potential to provide public good by facilitating access to health information for the purposes of public health reporting, bioterrorism event monitoring, disaster preparedness, health care quality improvement support, and research. What kind of information should be shared for non-treatment purposes? How should this sort of use be authorized and managed?

Redacting
In an electronic environment the ability to redact specially protected information from a health record is more complicated than in a paper world. How will personal health information be protected from improper sharing when health records are sent electronically?

Data transmission security
Electronic health information exchange will allow providers to send and review health information more easily, both internally and externally. Patients changing doctors or seeing specialists will no longer experience delayed care while waiting for records to be sent. What minimum standards need to be developed to ensure the technical security of electronic transmissions of health information? How can such standards be enforced? How do we assure all of Oregon's providers can appropriately participate regardless of their level of IT implementation?

Tracking access and audit trails
As health information is increasingly available electronically, it is important to do as much as possible to prevent the information from being inappropriately accessed or shared. However, in the event a breach of security does occur, it is essential to have a robust system of audit trails to track access to a patient's record so that appropriate steps can be taken to ensure the inappropriate access is detected and does not reoccur. What standards surrounding maintaining audit trails are needed? How can we learn from mistakes and continually improve the security protections of health information? What technical changes or developments are required to accommodate appropriate audit controls (especially with legacy systems)?

Increased liability
Improved health information exchange may result in large quantities of patient health information being sent to providers without an immediate tie to a visit for diagnosis and treatment. Will increased provider liability result from the creation of more information than can be reasonably used? Will healthcare organizations also experience greater liability? How should we address issues that arise from having too much or too little information?

Need for effective sanctions
In order to assure the public trust in healthcare organizations' ability to appropriately protect personal health information, a universal standard of accountability needs to be applied for individuals and/or organizations that violate the privacy and security of electronic health information. How can this be ensured? What are other ways to ensure the public trust? Despite all safeguards to protect security and privacy of health information, inappropriate disclosures will inevitably occur. What should happen when inappropriate disclosure (inadvertent or intentional) occurs? Who is responsible? How will privacy and security requirements be enforced?

4. Introduction to Analysis of Solutions

The health care environment is changing: electronic health records are replacing paper records and health information is increasingly being exchanged electronically. The electronic exchange of information has the potential to revolutionize health care in many ways including through improved quality, cost efficiencies, enhanced patient/consumer engagement, and greater continuity of care. While the technology to do this is emerging, there is still a great deal of work to be done to allow for a smooth transition into this new world.

To function in this new environment, trust relationships must be built between individuals and organizations involved in health care or the handling of health information. Multiple high-profile unintended, but inappropriate disclosures have heightened consumer concern for the privacy and security of their electronic health information. The need to protect individuals' privacy must be balanced with the need to share individuals' health information so that care is safe, effective and efficient. Achievement of this balance necessitates an approach that includes an enhanced role for the individual in determining the flow of their health information. It is in this spirit that the Oregon Health Information Security and Privacy Collaboration (HISPC) offers the following recommendations.[1]

The following values frame Oregon's policy for assuring the privacy and security of electronic health information.

Values

- **Trust**. All those involved in data exchange should earn and build trusting relationships among parties.
- **Privacy**. Individuals' information should not be shared beyond what is essential.
- **Autonomy**. Patients/consumers should be able to freely and independently (without coercion) make informed choices about managing their health and health information
- **Portability**. Patients/consumers should be able to get care wherever they choose; this choice should not affect the availability of their health information.
- **Equality**. The ability of providers and patients/consumers to access resources and information should not be dependent on economic, cultural, or other similar factors.
- **Feasibility**. Solutions should be realistic; funding and functionality should be considered.
- **Transparency**. The public must be able to see and understand how decisions are made and information is shared.
- **Public Accountability**. The public should have the awareness and the ability to require changes in the process if it is not meeting core values.
- **Balance**. Balance should be sought between potentially conflicting goals and values.

[1] It is understood that providers of healthcare services are required to keep records for purposes of medico-legal documentation. The recommendations of the HISPC do not disturb this requirement but pertain mostly to the record created or assembled as a result of information sharing *between* entities.

5. Review of State Solution Identification and Selection Process

The solutions presented in this report were developed by the SWG in open, discussion-based meetings. All members of the VWG were invited to participate in the meetings with additional invitations made to key stakeholders and topic experts. Representatives of consumer organizations were also asked to join the SWG particularly for the discussions of patient involvement and specially protected information. Project staff engaged a diverse group of stakeholders, continuing to invite people throughout process.

Each SWG meeting began with a brief introduction of the topic and presentation by staff. Participants were also emailed resources such as national research and resources and examples from other states specific to each topic prior to meetings. Staff often proposed a particular viewpoint (such as a stance taken by the author of one of the resources emailed out) with the goal of eliciting comment and discussion from the group. The majority of the two-hours allotted for each meeting was consumed by discussion as staff sought to generate as many opinions and solutions as possible. A recap by staff at the end of each meeting summarized the discussion and provided an opportunity to reach consensus on any of the proposed solutions.

Although the SWG was an open group with new members joining for every meeting, a core group emerged representing hospitals, providers, state government, health systems, payers, quality improvement organizations, and technology experts. The group was charged with discussing options to resolve the key issues raised, with an emphasis placed on open discussion rather than narrowing down the options. Solutions were identified by the SWG, Steering Committee and staff and brought to the entire group for feedback and comment.

All solutions have been prioritized by the Steering Committee based on feasibility and impact. Solutions with high impact and low barriers to feasibility will likely receive the greatest attention. However, the Oregon State Legislature is in session and priorities could shift based on the legislative agenda.

6. Analysis of Oregon Proposed Solutions

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

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

   - **General context:** 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.
   - **Proposed solution:** Identify appropriate statutory solutions to ensure the Markle principles are implemented in Oregon. Implement the Markle principles in HIE policy, architecture, and business agreements. Implement the principles in State programs, including the Public Employees Benefit Board, Medicaid, and state funded HIE pilots. Implement the principles wherever personal health information is exchanged.
   - **Coordinating responsibility:** Shared public-private partnership
   - **Domains:** All
   - **Types of HIE (clinical, public health, research) addressed:** The solution will address the exchange of clinical information, clinical lab, public health and research information
   - **Stakeholders primarily affected:** Providers, hospitals, physician groups, State government
   - **HIE barriers:** Patient engagement and trust
   - **Stage of development:** Proposed
   - **Extent to which proposed solution is in use:** Not currently in wide use
   - **Applicability of solution:** Applicable to other states and organizations
   - **Extent of barriers or opposition:** Cultural barriers and cost
   - **Type of solution:** Policy

2. **A coordinated approach to identifying, authenticating and authorizing <u>providers.</u>**
   - **General context:** 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.
   - **Proposed solution:** Engage the Oregon Medical Association, Oregon Association of Hospitals and Health Systems, Oregon Health Sciences University, and the Oregon Board of Medical Examiners in the design of a database that authenticates providers based on licensure credentials. Develop a standard approach to provider authentication and authorization that uses appropriate and feasible safeguards and technology. Engage vendor partners as appropriate and participate in national-level discussion as it evolves.
   - **Coordinating responsibility:** State government and private sector consortia
   - **Domains:** 1, 2, 3
   - **Types of HIE (clinical, public health, research) addressed:** The solution will address the exchange of clinical information, clinical lab, public health and research information

- **Stakeholders primarily affected:** Providers, hospitals, physician groups
- **HIE barriers:** Organizational differences
- **Stage of development:** Authentication database is in beginning stages
- **Extent to which proposed solution is in use:** Emerging in Oregon, present in other states
- **Applicability of solution:** Applicable to other states and organizations
- **Extent of barriers or opposition:** Cultural barriers and cost
- **Type of solution:** Technical, policy

3. **A coordinated approach to identifying, authenticating and authorizing patients.**
   - **General context:** 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.
   - **Proposed solution:** Review and analyze RAND study on patient identifiers. Review and assess use of Master person Identifiers. Evaluate existing systems for patient identification currently used at major provider and payer systems. Assess the issuance of voluntary patient ID numbers. Monitor and assess pilot group models. Adopt or develop a set of common standards or models for identifying patients within and across HIE systems. Develop a funding strategy to maintain the system. Assist in communicating needs to vendors and regional health information exchanges. Negotiate bulk purchase rates with vendors.
   - **Coordinating responsibility:** State government and private sector consortia
   - **Domains:** 3
   - **Types of HIE (clinical, public health, research) addressed:** All types
   - **Stakeholders primarily affected:** Providers and patients
   - **HIE barriers:** Organizational differences
   - **Stage of development:** Conceptual
   - **Extent to which proposed solution is in use:** Not currently in use
   - **Applicability of solution:** Applicable to other states and organizations
   - **Extent of barriers or opposition:** Cultural barriers and cost
   - **Type of solution:** Technical, policy

4. **An educated and engaged Oregon population regarding health information privacy rights and expectations.**
   - **General context:** 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.
   - **Proposed solution(s):**
     a. Develop plain-language HIE privacy and security practice descriptions to be used to inform and educate consumers
     b. 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
     c. Build statewide consensus on a uniform process for implementing participation permission form
     d. Develop and build a monitored process to ensure compliance with the uniform process for implementing participation permission forms for all HIE systems
   - **Coordinating responsibility:** Shared public-private partnership
   - **Domains:** Outside of domains
   - **Types of HIE (clinical, public health, research) addressed:** All types

- **Stakeholders primarily affected:** Consumers
- **HIE barriers:** Patient engagement and trust
- **Stage of development:** In progress
- **Extent to which proposed solution is in use:** Not currently in use
- **Applicability of solution:** Applicable to other states and organizations
- **Extent of barriers or opposition:** Cultural barriers and cost
- **Type of solution:** Education

5. **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**
   - **General context:** 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.
   - **Proposed solution:** Create a comprehensive list of current Oregon laws that pertain to privacy and security of health information. Identify model laws from other states and determine applicability to Oregon. Convene appropriate stakeholders and Privacy and Security Advisory Board to make recommendations for reform. Draft legislation coordinating with national models as deemed needed an appropriate. Ensure that explanatory materials are developed and disseminated pursuant to the Consumer Engagement Work Plan.
   - **Coordinating responsibility:** State government with private sector partners
   - **Domains:** 8
   - **Types of HIE (clinical, public health, research) addressed:** All types
   - **Stakeholders primarily affected:** All stakeholders
   - **HIE barriers:** Fear of violating rules or litigation
   - **Stage of development:** Conceptual
   - **Extent to which proposed solution is in use:** Not currently in use
   - **Applicability of solution:** Applicable to other states and organizations
   - **Extent of barriers or opposition:** Cultural barriers
   - **Type of solution:** Education

6. **An examination of state laws regarding identity theft to determine if medical identity theft is appropriately and adequately addressed.**
   - **General context:** 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.
   - **Proposed solution:** Monitor laws and administrative rules developed to ensure medical identity theft is addressed. Make recommendations to the Department of Consumer and Business Services. If appropriate, develop materials and recommendations for healthcare providers to educate them of the issue. Develop materials and recommendations for consumer education if appropriate. Coordinate across state agencies regarding identity theft legislation.
   - **Coordinating responsibility:** State government with private sector partners
   - **Domains:** 1, 2, 3
   - **Types of HIE (clinical, public health, research) addressed:** All types
   - **Stakeholders primarily affected:** All stakeholders
   - **HIE barriers:** Insufficient state law
   - **Stage of development:** In development
   - **Extent to which proposed solution is in use:**
   - **Applicability of solution:** Applicable to other states and organizations
   - **Extent of barriers or opposition:** Knowledge and awareness

- **Type of solution:** Legal

7. **Support to organizations for comprehensive adoption of appropriate *privacy* and *security* practices for HIPAA and other federal and state law compliance and contractual obligations.**
   - **General context:** 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.
   - **Proposed solution:** Develop best practice documents for privacy and security. Support the Oregon and SW Washington Privacy and Security Forum's and the Oregon Association of Hospitals and Health Systems' work in this area. Post the best practices on Q-Corp website and distribute across state. Identify audience and funding to distribute practices. Maintain and update the recommended practices. Support organizations adopting the practices administratively and technologically.
   - **Coordinating responsibility:** Public and private sector consortia
   - **Domains:** All
   - **Types of HIE (clinical, public health, research) addressed:** All types
   - **Stakeholders primarily affected:** Healthcare organizations and providers
   - **HIE barriers:** Insufficient education about privacy and security best practices
   - **Stage of development:** Conceptual
   - **Extent to which proposed solution is in use:** Not currently in use
   - **Applicability of solution:** Applicable to other states and organizations
   - **Extent of barriers or opposition:** Cost
   - **Type of solution:** Education

8. **Legal privacy and security requirements for entities handling personal health information that are not covered by HIPAA**
   - **General context:** 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 HIPPA covered entities participating in HIE
   - **Proposed solution:** Work in partnership with the Oregon Attorney General, who is a voting member of the State e-Health Alliance, the National Conference of Commissioners on Uniform State Laws and the Oregon Department of Consumer and Business Services to explore options with respect to legal standards for non-HIPAA covered entities. Engage vendors such as Omnimedix and WebMD to work on solutions. If determined to be necessary and appropriate, develop and implement legislation and regulations to ensure non-covered entities maintain appropriate privacy and security practices.
   - **Coordinating responsibility:** State government with private sector partners
   - **Domains:** 4, 5, 6, 7
   - **Types of HIE (clinical, public health, research) addressed:** All types
   - **Stakeholders primarily affected:** Non-covered entities and patients
   - **HIE barriers:** Misunderstanding of who is covered by HIPAA
   - **Stage of development:** Conceptual
   - **Extent to which proposed solution is in use:** Not currently in use
   - **Applicability of solution:** Applicable to other states and organizations
   - **Extent of barriers or opposition:**
   - **Type of solution:** Legal

9. **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**
    - **General context:** 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.
    - **Proposed solution:** Identify and define types of secondary use and develop model practices, policies and procedures for each type. Provide technical assistance to HIE efforts to aid adoption of appropriate secondary use practices. Coordinate with Institutional Review Boards to ensure their alignment with models.
    - **Coordinating responsibility:** State government with private sector partners
    - **Domains:** 9
    - **Types of HIE (clinical, public health, research) addressed:** Public health and research
    - **Stakeholders primarily affected:** State government, research
    - **HIE barriers: Stage of development:** Conceptual
    - **Extent to which proposed solution is in use:** Not currently in use
    - **Applicability of solution:** Applicable to other states and organizations
    - **Extent of barriers or opposition:** Cultural
    - **Type of solution:** Legal

10. **Legislative or regulatory measures to address inappropriate disclosures and mitigate potential harmful effects of personal health information disclosure**
    - **General context:** 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.
    - **Proposed solution:** Assess current State and Federal law which is being used or not used for enforcement. Review national model laws and enforcement mechanisms and evaluate applicability of these and current Oregon laws to the HIE environment. Develop and build a system to assist consumers in understanding their rights and the ability to seek redress when those rights have been violated.
    - **Coordinating responsibility:** State government with private partners
    - **Domains:** Outside of domains
    - **Types of HIE (clinical, public health, research) addressed:** All types
    - **Stakeholders primarily affected:** All
    - **HIE barriers: Stage of development:** Conceptual
    - **Extent to which proposed solution is in use:** Not currently in use
    - **Applicability of solution:** Applicable to other states and organizations
    - **Extent of barriers or opposition:**
    - **Type of solution:** Legal

11. **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**
    - **General context:** The State should support implementation and dissemination of the Health Information Security and Privacy Collaboration recommendations and Implementation Plan. These recommendations will foster protection of patients' personal information and the exchange of electronic health information as health information exchange evolves.
    - **Proposed solution:**
        a) Establish a Health Information Privacy and Security Advisory Board to advise the State regarding privacy and security
        b) 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
        c) Provide recommendations to state legislators and policy makers through analysis, briefings and testimony

d) Track and participate in the national discussion on HIE privacy and security issues to assure Oregon methods will align with national initiatives
e) Provide coordination for government programs that interface with the private sector
f) 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

- **Coordinating responsibility:** State government
- **Domains:** Outside of domains
- **Types of HIE (clinical, public health, research) addressed:** All types
- **Stakeholders primarily affected:** State government, health plans, hospitals/health systems
- **HIE barriers: Stage of development:** Conceptual
- **Extent to which proposed solution is in use:** Not currently in use
- **Applicability of solution:** Applicable to other states and organizations
- **Extent of barriers or opposition:** Cost and political will
- **Type of solution:** Government

7. National-level Recommendations

The solutions outlined in the preceding sections of this report represent the opportunity for Oregon to significantly improve privacy and security protections of personal health information within the state. Action on the recommendations will engender public trust and confidence in health information exchange. However, many of the critical issues creating barriers to health information exchange need national-level solutions. The Oregon HISPC team recommends the following national-level solutions be implemented.

National-Level Recommendation	Proposed National Implementers
Implement, through legislative or regulatory means, a patient consent/control requirement within HIPAA for all exchanges of health information.	Office of the National Coordinator (ONC), Department of Health and Human Services (DHHS)
Work to bring states together to create uniform state laws that reconcile differences between state and federal laws. Provide funding to the National Conference of Commissioners on Uniform State Laws (NCCUSL) to partner in this effort.	ONC
Elevate the conversation of privacy and security to the executive level of State government.	Alliance for State e-Health
Monitor the development of opt-in/opt-out approaches; consider local, regional, and provider variations; collect evidence on the health, economic, social, and other implications; and continue to evaluate in an open, transparent, and public process, whether a national policy on opt-in or opt-out is appropriate.*	DHHS
Create legislative or regulatory measures pertaining to entities that handle personal health information and are not covered by HIPAA requiring that at a minimum, legal standards at a level equivalent to HIPAA be followed.	DHHS
Implement a public awareness campaign that will help the public understand what they stand to gain with increased exchange of health information and how their health information will be protected.	ONC, National Governor's Association, Office for Civil Rights
Reevaluate the National Patient ID based on a thorough review and analysis of the RAND study on patient identifiers.	DHHS
Impose appropriate penalties for egregious privacy, confidentiality, or security violations committed by any individual or entity. Develop legislative or regulatory means to ensure that individuals whose privacy, confidentiality, or security is breached are entitled to reasonable compensation.*	DHHS
Require transparency regarding the secondary use of personal health information.	DHHS
Create a privacy certification process for HIE efforts	ONC

*From the National Committee for Vital and Health Statistics Letter to the Secretary; Recommendations regarding Privacy and Confidentiality in the Nationwide Health Information Network, June 22, 2006

8. Conclusions and Next Steps

The variation phase of the HISPC project provided the Oregon team an excellent framework to explore and analyze business practices pertaining to the privacy and security of health information exchange in Oregon. Discussions of the scenarios revealed limited variation in practice, but substantial common critical issues facing all entities that exchange personal health information. The rest of the project centered on this list of critical issues, as the Solution and Implementation Plan Work Groups wrestled with contrasting and often conflicting priorities.

The solutions presented in this report provide direction for future work in Oregon to protect individual privacy and security and earn the public trust necessary to make health information exchange work for Oregon. The next steps for Oregon, detailed in the Final Implementation Plan, represent an opportunity for partners across the state to work together to deliver on the promise of health information exchange.