



# Metropolitan Portland Health Information Exchange
# Security & Privacy 2.5

## Results and Reports Retrieval System

Last Updated: 6/5/2007 3:06 PM

Contacts:

Densie Honzel, Oregon Business Council Consultant, honzelde@aol.com

Nancy Clarke, Oregon Health Care Quality Corporation Executive Director, nancy.clarke@Q-Corp.org

TABLE OF CONTENTS

## Introduction & Summary

The objectives of the Security & Privacy Assessment 2.0 are:

- Amplify and update the key security and privacy requirements for the health information exchange as identified in the Early Deliverables (Security & Privacy 1.0).
- Identify key trends and sources of Privacy & Security best practices nationwide.
- Understand the rapidly-evolving policy debate that is presenting strong challenges to the design of viable health information exchanges across the country.
- Evaluate and incorporate legal requirements (HIPAA, other federal law and state law, specifically addressing specially sensitive information)

The metropolitan Portland HIE will succeed only if it addresses issues of privacy and security in a balanced and patient-friendly manner. This project will only be successful if both consumer and providers (and potentially health plans) are comfortable with information sharing across multiple entities. Fortunately, there are several important sources of information about security and privacy in HIE at the state, regional and national levels. Based on review of the local environment and national trends, the following recommendations should be taken into account during the design and implementation of the Portland HIE.

- **Patient Consent:** Some level of consent is absolutely necessary to make HIE work in the region. At a bare minimum, patients must have a meaningful opportunity to opt out of the HIE. However, it is strongly recommended that the HIE adopt a policy active consent (opt in) to enroll patients.
- **Privacy & Security Services:** The HIE should provide a hybrid of central and distributed services for Authorization, Authentication, Access, Audits, Risk Analysis, Risk Management, etc. Models exist for the provision of strong, lightweight model for these services. The HIE should be constructed to industry-standard levels of administrative, physical and technical security that also meet federal and state legal requirements.
- **Oregon HISPC Recommendations:** The Portland Metro HIE Privacy and Security plan should be informed by the Oregon HISPC recommendations to provide for the solutions described in Appendix A.
- **Technology Strategy:** The clinical and business requirements for the HIE resulted in a technology strategy based on a hybrid of federated and centralized architecture. This allows a gradual expansion and phase-in of services over time to result in a sustainable HIE. The privacy requirements should likewise be

phased in relation to services provided, while supporting the necessary patient consent requirements. Also, any technology infrastructure decisions made should take into account current standards being selected by HITSP.

- **Governance & Management of Privacy & Security:** A Privacy & Security Council should be established within the governance model to develop the overall privacy and security plan for the HIE. The Council will vet the rules, contracts/legal agreements, description of use (e.g., treatment, payment, healthcare operations, secondary use, release for public health purposes, etc.) and SOPs for the exchange. It will oversee privacy and security aspects of technical implementation, remedy "exceptional" events that might constitute a breach of privacy or inappropriate access, provide appropriate security and privacy management so as to address legal requirements (federal and state) and act as "ambassadors" for privacy & security aspects of the HIE, to the public and participating organizations throughout the community.

Privacy and security considerations may appear to slow the development of the Portland Metro HIE on the surface. Adoption may proceed more slowly with an opt-in model, it may take longer to realize the projected financial benefits and users may initially realize less clinical value from the exchange. However, the enduring success of the project depends on "getting it right the first time" so that patients and the participating providers trust the HIE enough to allow the community to obtain the enormous potential benefits in the long run.

## Background & Sources

The lack of robust security and privacy policies surrounding health information exchange (HIE) are a topic of furious national debate[1]. It has been recognized that while efforts to date focusing on standardization and technical implementation of HIE networks has been proceeding quickly, there has been less than the needed amount of attention applied to issues of managing health information in a way that is consistent with patients' desire to keep information confidential, secure and limited as to access. As such, the attention given to security and privacy of HIE has accelerated at the national and local levelsin the Winter and Spring of 2007; it is widely recognized that the success of HIE efforts locally and nationally are critically dependent on appropriate privacy and security practices (administrative, physical and technical).

As discussed below, Portland must necessarily go beyond applying a baseline enforcement of HIPAA, Oregon law and other applicable federal law to the HIE; rather, the new environment posed by the digitization and sharing of healthcare information poses unique situations and challenges for the management of access to that information. There is a need to develop a comprehensive and unifying framework for privacy and confidentiality at the national and state levels. To date, none of the US Department of Health and Human Services commissions have put a credible stake in the ground in this area. The metropolitan Portland HIE should not move forward with the exchange of health information without establishing the necessary privacy and security protections first. In particular, the issue of patient control over access to information in the exchange must be dealt with before day one of HIE operations.

There are several important sources of information to assist in developing a standard security and privacy infrastructure when designing and implementing a health information exchange. This document summarizes relevant findings from the following sources:

1. Health Information Security and Privacy Collaborative (HISPC) project – National & HISPC Oregon
2. Nationwide Health Information Network (NHIN) Forum #2 and Forum #3
3. National Committee for Vital and Health Statistics (NCVHS) Requirements for health information exchange
4. Results of surveys and focus groups from other regions – Florida, Tennessee, and Rhode Island.

[1] Sloane, T (2007). Privacy could be IT standards' deal-breaker. Modern Healthcare Online, http://www.modernhealthcare.com/apps/pbcs.dll/article?AID=/20070309/FREE/70308003/0/FRONTPAGE. Accessed 3/12/2007.

5. The Health Information Management Systems Society (HIMSS) Annual Meeting 2007, particularly the RAND Study on Patient Identifiers.
6. The National Institute for Standards & Technology (NIST)
7. International Standards Organization (ISO; specifically ISO 17799)
8. The Workgroup for Electronic Data Interchange (WEDI)

## National Health Information Security and Privacy Collaboration (HISPC)

The U.S. Department of Health and Human Services (HHS) Agency for Health Research and Quality (AHRQ) and the Office of the National Coordinator for Health Information Technology (ONC) commissioned RTI International to identify appropriate practices and develop solutions to overcome variances in laws and business practices that prevent state and nationwide sharing of electronic health information while continuing to protect patient and health plan member privacy and security. This project involved subcontracts to 34 states and territories to help assess and develop plans to address variations in organization-level business policies, state laws and federal laws that affect privacy and security practices which likely pose challenges to interoperable health information exchange. Some interim results of the national HISPC work are available on the web at http://www.rti.org/hispc.

This section summarizes findings from national debates, conversations occurring in Oregon and conversations occurring in other states. A wide variety of experts, including consumers, have been engaged in the discussion. These include not just clinicians, medical records staff, and healthcare technologists, but also thought leaders in privacy and security law and health care management. There are three main areas of high concern covered in the current document:

- Patient Consent
- User Authorization/User Authentication/Data Access/Auditing
- Data Security

### Patient Consent

In the area of patient consent, there are a wide variety of possible approaches to managing the granularity and situations in which consent is required. The RTI/HISPC project reports that consumers are chiefly concerned about three things when thinking about consent[2].

- Consent should be meaningful and their wishes respected.
- Consumers want assurance that their information will be seen only by those whom they authorize.

[2] Quarrier, JO and Colello, A (2007). Federal and New York State Consent Laws Re: Disclosure to HIEs - Now and Into the Future. Privacy and Security Solutions for Interoperable Health Information Exchange National Conference. http://www.rti.org/files/hispc/hispc_TrackA_Day1.pdf. Accessed March 12, 2007.

- Consumers want to know that the system will be secure to reasonably ensure inappropriate disclosure does not occur.

A moderate "hybrid" approach was presented to govern consent in a regional exchange. In this approach, a general consent plus notice is sufficient to load general information about the patient demographics and clinical information into the exchange. However, specific authorization is required to exchange specially-protected (a.k.a. "sensitive") information[2] as defined by Oregon and federal law. A framework to support this approach is proposed below in the sections on Technology and Operations.

**Authorization, Authentication, Access and Audits**

The most technically salient areas of privacy and security in HIE are concerned with the 4 A's – Authorization, Authentication, Access and Audits. The national HISPC project provided important findings on these topics[3]. The following summarizes the key findings in the form of requirements for a health information exchange.

- *Authentication:* provide appropriate and strong authentication for direct access to the exchange (this could mean multi-factor authentication). Single-factor authentication may be permissible from within a trusted entity or domain depending on the risk level the organization is willing to accept (e.g. a health system participating in the exchange).
- *Access Control:* Providers should only access information for patients with whom they have a treatment relationship. Exceptions, such as in the event of an emergency, need to be accommodated through what has been termed "break the glass" which allows the provider access but generates a report of access that is forwarded to the patient's primary care physician. Access control should also include management of access. In other words, an individual or group of individuals need to be granted the authority to grant and revoke access and manage that access.
- *Authorization:* Security credentialing guidelines should include the ability to verify the identity of individuals authorized to access or exchange information; define role-based access for individuals; and manage the authorization process.
- *Auditing:* Minimum standards for routine auditing. (NOTE: This could include auditing of information upload, viewing/download, modification, or deletion of data).

  Auditing includes regularly scheduled audits examining audit logs generated related to specific activities such as viewing or changing

[3] Golden, J (2007) Framework for Addressing the 4As. Privacy and Security Solutions for Interoperable Health Information Exchange National Conference. http://www.rti.org/files/hispc/hispc_TrackB_Day1.pdf. Accessed March 12, 2007.

PHI, an annual audit that addresses policy and procedure compliance, review of risk mitigation activity when identified through a regular risk analysis, review of the disaster recovery plan to determine if it is current and complete, etc. Auditing needs to include the technical component that accommodates generation of appropriate audit logs of system and individual activity.

There is strong support nationally (from HISPC, from the Health Information Technology Standards Panel (HITSP), and from the EHR Vendors Association) for the continued development and implementation of Integrating the Healthcare Enterprise (IHE) profiles related to access, authentication, authorization and auditing. The following integration profiles have direct bearing on the above:

- Audit Trail Log and Node Authentication (ALNA)
- Patient Identity Cross-Reference (PIX) and Patient Demographic Query (PDQ)
- Consistent Time

While not all of these profiles are requirements of the system, they do provide meaningful examples of how privacy and security issues can be resolved with a well tested set of standard approaches. It should be noted that generation of audit logs that are examined is a requirement of the HIPAA security rule.

**Information Security**

Key elements of information security not already covered above include the following[4]:

- *Encryption & Integrity:* Protection of data in transit and at rest, and assurance that data rendered for viewing is complete and correct.
- *Physical Security:* Standard operating procedures for management of physical access to data centers, networks, hardware systems, facilities, media, workstations (desktops and laptops, etc.) and appropriate contingency planning including disaster recovery planning and emergency mode operations planning.
- *Administrative Security:* The development, implementation and enforcement of appropriate policies, procedures and practices that relate to access control, authentication, access management, training, information systems activity review, auditing, etc.
- *Technical Security:* Deployment of firewalls, anti-spyware and anti-virus software, secure web access (use of encryption), technical methods of authenticating a user, generation of audit logs, deployment of intrusion detection or prevention systems,

[4] Hack, L and Holm B (2007). Adoption of Common Privacy & Security Standards Session 3B: Trust in Security. Privacy and Security Solutions for Interoperable Health Information Exchange National Conference. http://www.rti.org/files/hispc/hispc_TrackB_Day1.pdf. Accessed March 12, 2007.

patch management process, application security functionality analysis, etc.

## Oregon HISPC Project

Oregon received one of the subcontracts for states from the AHRQ/ONC sponsored HISPIC project through a request for proposal (RFP) process jointly managed by the National Governors Association (NGA) and RTI International (the national project contractor). It has been administered through the Governor's office and the Office for Oregon Health Policy and Research (OHPR). The Oregon HISPC project convened technical, legal, medical, health insurance, government, consumers and health policy expertise to assess variations in practice and develop solution recommendations. The mission statement for the project is:

> *"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."*

The preliminary results of the Oregon HISPC solution recommendation are included in Appendix A of this document and are available on the web at http://www.q-corp.org/q-corp/images/public/HISPC/Solution%20Recommendations%20draft.pdf.

Briefly, the Oregon HISPC project team with the approval of the project executive steering committee recommended adopting the Markle Foundation principles outlined in the full document referenced above. The principles relate to guaranteed convenient and affordable access to health information, control over whether and how personally identifiable health information is shared, how information is used and who has access to it, protection of the integrity, security, confidentiality and appropriate availability of information, transparency and accountability of HIE governance.

The Portland Metro Health Information Privacy and Security requirements should be informed by the Oregon HISPC project recommendations to address initially for the following nine "solutions" detailed in Appendix A:

1. Provider Identification, authentication and authorization.
2. Patient Identification, authentication and authorization.
3. Public Engagement.
4. Specially Protected Information.
5. Medical Identity Theft.
6. Technical Assistance.
7. Non-Covered Entities.
8. Secondary Use.
9. Enforcement.

In summary, the Oregon HISPC project will assist Oregon to move in the direction that reasonably ensures it is consistent with emerging national standards while also highlighting special requirements that may be unique to the state and region.

## Nationwide Health Information Network (NHIN) Forums

The Nationwide Health Information Network (NHIN) Forums were designed to provide updates on the work of the various subcommittees of HHS focused on health information technology (IT), advance discussions and develop clarity regarding architectural approaches to reasonably ensure security and privacy, showcase the work of the four NHIN Consortia by providing an opportunity to see actual demonstrations of health information exchange prototypes, and promote discussion on different approaches to business models that target establishment of self sustaining health information service providers and exchange.

The 2nd NHIN forum in October 2006 was focused on the functional requirements for security and privacy. The following discussion summarizes the technical aspects of authentication and authorization, including different approaches to each[5].

*Authentication:* Authentication is a mechanism of determining that an individual, entity or system interacting with a network is who they claim to be. Credentials such as username/password, or other identifying information about a user (e.g. biometrics, smart cards, digital certificates, etc.) may be used for authentication. There are three main approaches to authentication under development. One is to authenticate the organization or "domain" that is trusted to access the network. All users authorized to access that domain are allowed to access the network (but not necessarily any data on the network). This is sometimes referred to as "node authentication." A second approach is to authenticate each provider or user of the network individually. A third approach is a hybrid of both of the previous two methods of authentication.

*Authorization:* Authorization is granting permission to request information or perform a function on the network. Authorizations may be provided on an individual basis or according to roles (e.g. physician) that are applied to groups of users. Assertions about the identity of the user, requester, and requester organization usually accompany the authorization, requiring a high degree of trust between entities in the HIE. Authorization is as much an administrative as a technical construct. An individual or organization needs to be assigned to manage access control and authorization.

[5] Huff, S, Ocasio, W, Kailar, R, and Jenkins, LJ (2006). Approaches to Provider Authentication and Authorization. 2nd Nationwide Health Information Network Forum: Functional Requirements. http://www.hhs.gov/healthit/nhin/forum_oct2006.html. Accessed 3/13/2007.

The rules surrounding authorization may be applied in various ways. Either the trusted organization or individual requesting information, the data provider (source) or a centralized security service may apply the rule. The centralized approach creates a thicker shared service layer for the community HIE, but it may make it easier to maintain granular global access rules governing PHI access and provider the patient with greater ability to control access to his/her medical record through the use of restriction requests. Support for granular segregation of data is still not mature.

The requirements for user identity management are influenced by technical constraints, consumer needs and physician behavior and preference. Following is a list of notable functional needs for user authentication and authorization of a regional HIE:

- Reduction of provider liability and risk.
- Disclosure of data needs to be appropriate to the requirement of data use.
- Identity management must have minimal impact on resources in the provider office or facility while continuing to accommodate strong authentication mechanisms.
- There must be minimal hassle factor and workflow interruption. For example, a single sign-on enabled by a federated identity management system is desirable, and requires appropriate security controls given the increase in risk associated with the implementation of a single sign-on system.
- Enforcement of variances from what the public and private sector ahs determined to be acceptable practice should be consistent.
- A single unique identifier for a physician is probably required and is currently being implemented nation-wide (HIPAA national provider identifier (NPI).

During the 3rd NHIN Forum in January 2007, it was widely recognized that consumer trust and public acceptance of health information exchange were issues that have not been fully dealt with. There were demonstrations of cross regional data sharing by for consortia of vendors working with communities. These demonstrations were credible evidence that information can be exchanged within and between communities, given the appropriate technical infrastructure, standardized rules and, where inter-state communication occurs, appropriate accounting for state legal differences addressed.

In all four prototype demonstrations, patient control was a core theme. In particular, there were many examples of the requirement for patients to “Opt-in” to participation in the HIE; a need to enable specific, granular control of information access/availability; allowance for “break glass” functionality in emergencies, and access audit procedures for the patient to understand who has seen the data. Likewise, there was a discussion that clinicians may need

notifications that data exists or is hidden from view by patient preference or legal requirement. It is likely that the degree to which patient control was addressed in the NHIN consortia demonstrations, it was in response to late-breaking critical requirements due to the rising profile of privacy and security concerns.

## NCVHS Requirements

The National Committee on Vital and Health Statistics (NCVHS) presented an update on its functional requirements for the NHIN in October 2006[6]. NCVHS' charge is to digest information gathered from the various NHIN Forums, seek public and expert input and define/recommend a minimum, inclusive set of requirements. The requirements were to focus on privacy and security and not intended to constrain architecture. A large list of requirements was whittled down to 11 high-level functional requirements intended to account for architectural variation due to different business cases, policy needs, maturity and consistency of standards and available technology.

**NCVHS/NHIN Functional Requirements Overview**

1. Certification – core capabilities required for participation.
2. Authentication – systems, software, entities, individuals.
3. Authorization – manage permissions/authorization to share information about location of health information or access to specified information. Permit aggregation & de-identification.
4. Person ID – uniquely identify an individual by a patient matching or correlation process, and specifications on tolerance of duplicate patient matches.
5. Location of health information – functionality to determine where records exist for a patient.
6. Transport & content standards – content, vocabulary, code sets, transport protocols, metadata, etc.
7. Data transactions – rules governing trigger events for information transmission, notification, disclosures, and emergencies.
8. Audit/logging – connections/disconnections to network services, notifications of access.
9. Time sensitive data access – request/response interactions with specific target systems, e.g. immunizations and medication lists.
10. Communications – HITSP-selected standard content & message formats.
11. Data Storage – aggregation from various locations, temporary or permanent repositories.

[6] Cohn, S and Reynolds, H (2006). Update on initial NHIN Functional Requirements from the National Committee on Vital and Health Statistics (NCVHS) Ad hoc NHIN Working Group. 2nd Nationwide Health Information Network Forum: Functional Requirements. http://www.hhs.gov/healthit/documents/PlenaryNCVHSCohnReynolds.pdf. Accessed 3/13/2007.

Though the NCVHS and HISPC seem to be gathering requirements on the same domain, the two efforts have planned to coordinate efforts.

## Summary of Privacy & Security Requirements

| ID | Requirement |
|---|---|
| 1. | Comply with HIPAA and Other Federal law – the HIE may operate as a "non-covered" entity, however information will be managed according to the rules applying to covered entities. The HIE is considered a business associate and therefore is required to enter into a business associate contract with all participating covered entities. |
| | |
| 2. | Comply with all Oregon patient privacy laws |
| 2.1. | Manage specially protected data according to Oregon law |
| | |
| 3. | Comply with a minimum agreed-upon set of privacy & security standards (administrative, physical and technical) established by the participating/governing stakeholders. |
| 3.1 | Create or adopt a definition of security and privacy standards; standard policies, procedures and practices; a minimum technical infrastructure, etc. that participating organizations agree by contract to adhere to prior to participation in the exchange and include provisions that specifically identify audit practices and sanctions for violation of commonly established standards. |
| | |
| 4. | Comply with all regulations and appropriate practices for administrative, physical and technical security of health information that have been agreed to by participants in the HIE. |
| 4.1 | Ensure data encryption in transit |
| 4.2 | Assess integrity (completeness and correctness) of rendered data |
| 4.3 | Examine risks and encrypt data at rest if appropriate |
| 4.4 | Perform regular risk analysis,. |
| 4.5 | Establish disaster recovery plans |

| | |
|---|---|
| 4.6 | Create emergency mode operations plans |
| | |
| 5. | Implement robust methods for patient consent processes that allow access to their health record and to be actively involved in making decision regarding who data is exchanged with in the exchange. |
| 5.1. | Allow patient to receive notification that their data may be included in a data exchange |
| 5.2. | Allow patient to opt out of the data exchange |
| 5.3. | Allow patient to view their own data in the exchange |
| | |
| 6. | Audit trails - Patients must be able to obtain information about how their data has been accessed via the exchange (audit trail), to guard against inappropriate disclosure. |
| 6.1 | Patient may view a report of who accessed data, when, and from what location. |
| 6.2 | The exchange will audit all user access, modification, addition, etc. to data exchanged on the HIE. |
| 6.3 | Hold individual users accountable for inappropriate use or disclosure of patient information |
| 6.4 | Protect individual users against excessive liability for disclosure |
| | |
| 7 | Patient consent of providers |
| 7.1 | Patient consent to allow specific providers or entities to view their health information. Allow patients to control who can access their data via the exchange. |
| 7.2 | Add/amend/annotate/dispute data in the exchange |
| | |
| 8. | Permit advanced patient control over data inclusion & access |
| 8.1 | Allow the patient to selectively prohibit specially-protected or sensitive data from inclusion in the exchange. |
| 8.2 | Allow the patient to selectively prohibit “other” (not specially-protected) data from inclusion in the exchange |
| 8.3 | Allow the patient to authorize only specific providers or entities to view sensitive or “other” data |

| | |
|---|---|
| | from within the exchange. |
| | |
| 9. | Enable role-based access control of providers and other authorized users of data |
| 9.1 | Role-based access control may be managed centrally or in a federated manner or both |
| | |
| 10. | Provide for robust authentication mechanisms of providers and other users of data |
| 10.1 | If accessing the HIE from within a trusted domain/node, single-factor authentication is permitted |
| 10.2 | If accessing the HIE from outside a trusted domain/node, require multi-factor authentication |
| 10.3 | Utilize a Single Sign-On for users and implement appropriate security controls that mitigate risks associated with single sign-on |
| | |
| 11. | Identity Management |
| 11.1 | Provide a mechanism to uniquely identify all providers/users of the exchange |
| 11.2 | Provide a mechanism to reliably identify an individual whose health information is part of the exchange. |
| | |
| 12. | Secondary Uses |
| 12.1 | Permit secondary uses of de-identified or pseudonymized patient information for research, public health, and quality improvement |
| 12.1 | Permit re-identification of patients in emergency cases only related to public health or community safety and permitted by law |
| | |

## Technology Strategy

The overall technology strategy for the Metropolitan Portland HIE is given in Section I of the mid-deliverables. For clarity, diagrams from the technology strategy for Stage 1 "Lite" and Stage 3 "Full Services" are replicated here. The technology strategy is phased in concert with the financing and sustainability mechanisms – the architecture allows expansion from initial functions that enable community benefits to the richer value-based services that come in later phases. Likewise, the functionality to support the needed security and privacy features of the exchange will be adapted and phased in over time but required privacy and security features will be implemented prior to the HIE "go live" date.

The architecture model shown in Figure 1 is a pure federation of data repositories or gateway servers residing at the health systems, together with lightweight centralized services for patient and provider identity, security management (authorization & authentication), and audit trails. In a federated model, the data initially resides with providers and the exchange HIE performs patient demographic queries, record location, and data query from the provider. The HIE temporarily aggregates the data for a specific individual and presents it to the requestor.

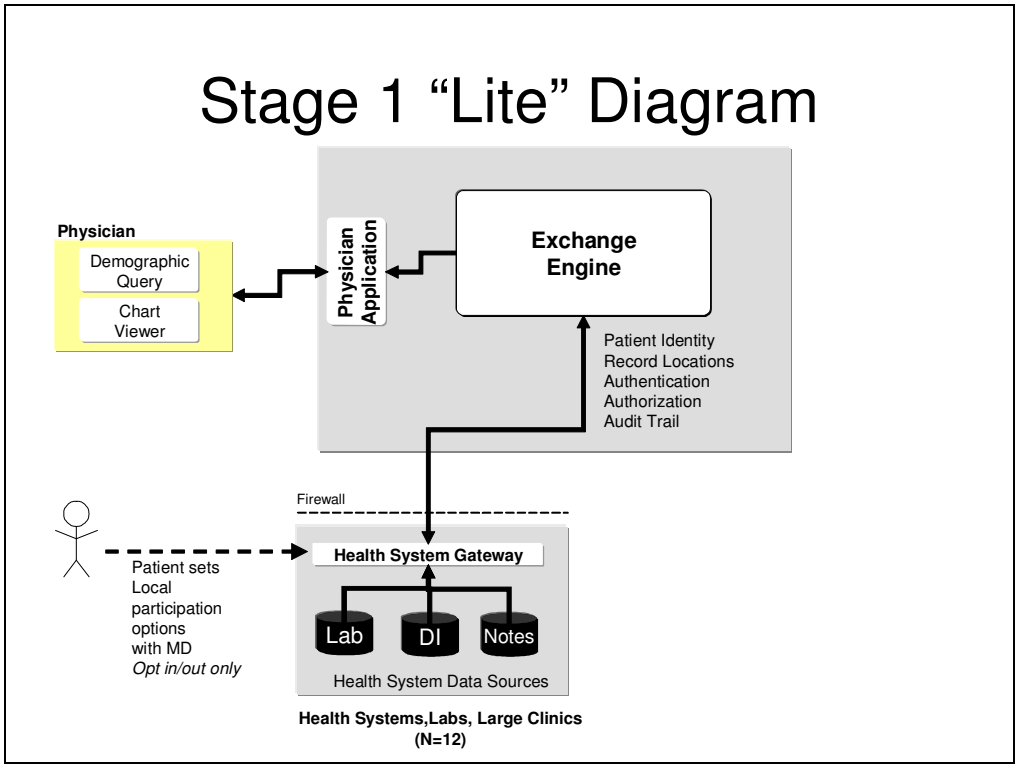


**Figure 1. Pure Federation of Data Sources.** The health system shown at bottom connects to the HIE via a gateway server. The gateway contains copies of the data that the patient has authorized to participate in the exchange. The patient works with the local provider to set participation options in the HIE; opt-in or opt-out, and whether "normal' and/or sensitive clinical information is accessible via the exchange.

Patient records are linked from their various sources by a matching algorithm that associates data for a specific patient identity. This is usually done with a master patient index (MPI; For a discussion of various approaches to identity, please see Appendix C.) In the federated model, consent must first occur in consultation between the patient and their originating provider in order for the patents' demographics and data to be registered with the exchange. In case the patient does not wish to participate in the exchange, or seeks to withhold selected data from being registered in the exchange, the provider would notify the gateway server at the health system to filter that patient's information according to their consent preferences as expressed at the local practice.

A second more granular level of consent could be configured to occur within the exchange. By allowing the patient to set global preferences for the exchange and registering those preferences centrally with the exchange engine, the patient could determine which other providers or locations would be able to access data for that patient from the exchange. Figure 2 shows a Patient application with "Exchange Participation Options" capability.

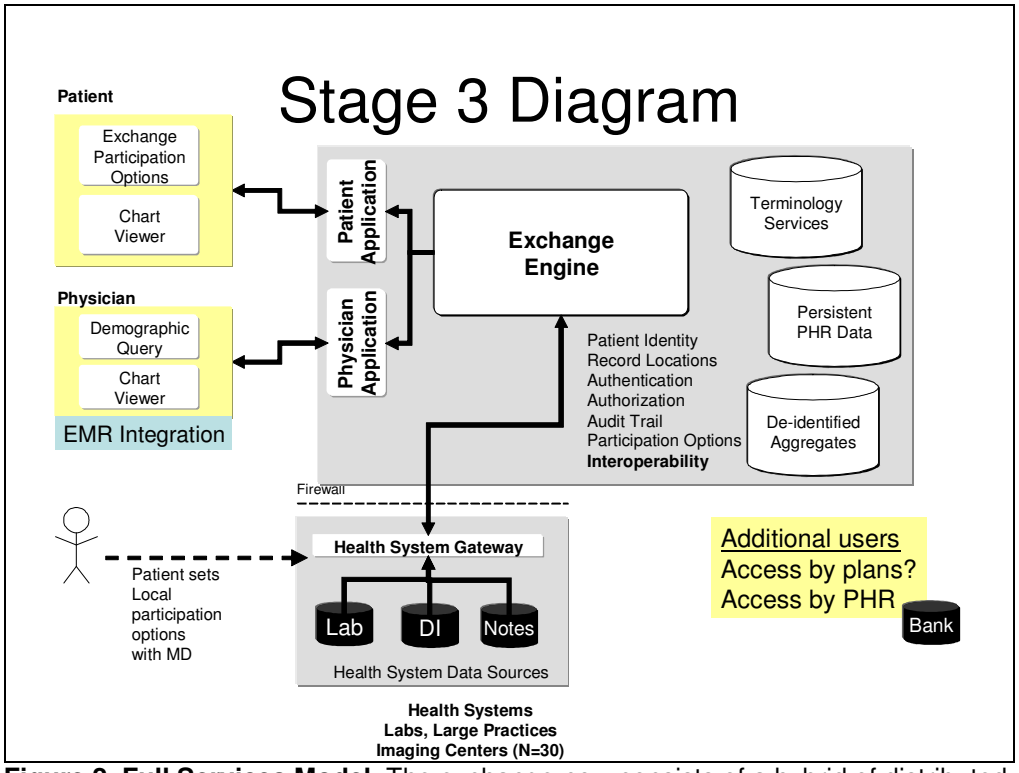


**Figure 2. Full Services Model.** The exchange now consists of a hybrid of distributed and centralized repositories of information for different purposes. The patient still has the capability to set participation options in the HIE with the local provider. In addition, the patient can access an application to set global participation options in the exchange, view the chart, and inspect audit logs.

Note that this second model assumes that the gateway has the capability to filter detailed patient information and selectively register certain data with the

exchange. It may be impossible to selectively redact sensitive information that is contained in a discharge summary or ED summary.

The patient application also includes a chart viewer whereby the patient can see what data about them is available through the HIE. The Patient Application would also allow viewing of audit/access logs to obtain details about who had viewed that individual's information via the exchange.

Note that under the models described above, there is not a universal, automatic opt-in to the exchange. Participation requires an explicit registration by the patient as opposed to a global batch registration of all patients who have not opted out. Therefore, emergency access to a patient's information under a "break the glass" scenario would only retrieve the data that the patient has allowed to participate in the exchange. If the patent set local options with a provider to exclude all or part of their encounter information or results from the HIE, then it would be impossible for anyone to retrieve that data using the HIE.

It would be possible to take the opposite approach using the same technical architecture; that is, to proactively register all patient information in the exchange, while performing the majority of access control and authorization centrally as depicted in Figure 2. In that case, a break the glass procedure would allow the emergency provider to view all data for that patient via the exchange. Stage 1 "Lite" shown in Figure 1 does not support this latter scenario, since there is no centralized management of authorization and access.

## Operations Strategy

There will necessarily be a division of labor for the privacy and security functions of the exchange. While the HIE operations team can manage some aspects of the global functions that are easily automated, there will be a significant responsibility on the part of the patients in consultation with providers to understand the participation options and implement the consent decisions in the exchange.

### Patient Consent

The exchange should develop standard materials that the participating providers can use to delineate rights and set expectations with the patients. The consent process should be as lightweight and standardized as possible, while ensuring that the patient's wishes are met, legal and are technically feasible. It will first be the provider's responsibility to reasonably ensure disclosure of patient information is appropriate (as long as technically feasible) and secondly the responsibility of the exchange when global participation options become available. It is often stated that "consent is fluid." Ideally, a kiosk or online consent process requiring patient authentication would be available so that the patient can review the HIE

policies and procedures at any time, and modify consent at any time. At the same time, it is desirable to minimize the burden on the provider office and administrative tasks required to participate in the exchange should be minimized.

**User Authorization/User Authentication/Data Access/Auditing**

User authorization with be a joint process involving the provider organization and the HIE operations team. In the case of the health system, it is assumed that the provider has current, role-based access to the health system network, such that access to the exchange (with possible single-factor authentication) is appropriate. The exchange may also register providers who are independent of the health system and offer them credentials to view patient information for which they are authorized. In this case the HIE would be responsible for a single level of user authentication, and data access would occur according to the patient's global options. The HIE would be responsible for auditing all network connections and disconnections, as well as the date time and identity of any access to a patient's information.

**Information Security**

The gateway server's communication with the exchange must necessarily be encrypted. Physicians would also view data in the exchange via an encrypted browser session. Data integrity would be ensured by a collaboration between the health systems as definitive sources of the data, the vendor of the HIE infrastructure and technical staff of the HIE operations. It would be the responsibility of the exchange to ensure that technical implementation of the gateways and HIE infrastructure conform to best technical security practices.

Common privacy and security standards, including a certification document, would be developed by the HIE operations staff in collaboration with the board of directors and technical advisory committee for the HIE. The rules and SOPs of the exchange would likewise be defined a priori with the Security and Privacy Council of the HIE board (see Governance Plan 1.0).

The exchange operations team and any service provider should be responsible to the auditing/detection of "exceptional" events that might constitute a breach of privacy or inappropriate access. The HIE board and/or Security/Privacy Council would be responsible for enforcement and remedy of exceptional events.

It will also be the responsibility of the exchange to ensure that secondary uses of data are in accordance with individual patient preferences and legal requirements. While there is not current requirement under HIPAA to seek patient consent for the use of fully de-identified data in aggregate form for secondary purposes, it is highly recommended to seek explicit patient permission for secondary uses in the exchange.

Other operational activities will include regular risk analysis, disaster recovery plans, and emergency mode operations plans.

## Implications for the MPHIE

The recommended privacy plan will have implications for the stakeholders, in that some of the potential uses of information envisioned by the participants may need to be delayed or deferred indefinitely. This particularly may apply to secondary uses. Also, there may be some privacy related challenges to the full realization of benefits projected in the Financial Plan 1.0. For example, if patient participation is low or if there is a significant amount of data that does not participate in the exchange due to patient preferences, the overall value of the exchange to the participating providers and health plans could be reduced.

The governance of the exchange must necessarily be responsive to – and ultimately responsible for – the execution of the privacy plan. The execution team that manages the operations of the HIE, together with the Privacy & Security Council and Board of Directors, must serve as ambassadors as well as hands-on technical liaisons to the participating organizations throughout the community.

We have attempted here to assess the challenges and focus on known "trigger points" that have been discussed nationally, regionally and at the state level that could yield a make-or-break outcome for the exchange. We have also suggested a technical approach to address those critical points in a way that gives the HIE the highest possible chance for success. There will be no substitute for a well-thought out and thoroughly vetted privacy and security plan for the Metropolitan Portland HIE. This effort will only succeed with consumer acceptance and comfort that the information in the exchange is primarily for the medical benefit of individuals.

## Appendix A: Recommended Solutions from the Oregon HISPC Project

Full document available at: http://www.q-corp.org/q-corp/images/public/HISPC/Solution%20Recommendations%20draft.pdf

**1. Provider Identification, authentication and authorization.**
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 essential to the success of HIE efforts. 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.
Activities: Develop models for applying the National Provider Identifier and for incorporating providers without NPIs into the systems. Develop models for consistent processes to be used across organizations, HIE systems, regions, and nationwide. Obtain agreement on models and implement.
Responsibility: Private sector consortia
Anticipated Timeframe: 18 months

**2. Patient Identification, authentication and authorization.**
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.
Activities: Convene partners to evaluate existing standards for patient identification. Adopt or develop a set of common standards or models for identifying patients within and across HIE systems. Assist in communicating needs to vendors and regional health information exchanges.
Responsibility: Private sector consortia
Anticipated Timeframe: 18 months

**3. Public Engagement.**
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.

Activities: Conduct consumer focus groups to engage consumers in a dialogue about expectations of consent within HIE and the best ways to communicate with all consumers in a quickly understandable way. Develop a consent form and process. Ensure the adoption by HIE efforts of the individual-centered approach recommended by the Markle Foundation Connecting for Health principles. Convene statewide conversations regarding public engagement. Develop a carefully monitored process to be followed each time an HIE system is implemented. Engage the press to cover the work of HISPC. Publish the HISPC reports and plan conferences to engage all partners in creating HIE in Oregon.
Responsibility: Shared Public-Private partnership
Anticipated Timeframe: Now and ongoing

**4. 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
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.
Activities: Examine current Oregon laws. Coordinate with national models and across states to develop consistent laws to ensure that HIE systems can appropriately protect and communicate information.
Responsibility: State government, with private partners
Anticipated Timeframe: Next legislative session

**5. Medical Identity Theft**

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.
Activities: Coordinate across state agencies regarding identity theft legislation. Monitor national developments surrounding the issue. Develop relationships with interested consumer groups. Coordinate with HIE efforts to help them understand and implement legal requirements.
Responsibility: State government, with private partners
Anticipated Timeframe: Current legislative session

**6. Technical Assistance**

Support to organizations for comprehensive adoption of appropriate privacy and security practices for HIPAA and other federal and state law compliance
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.
Activities: Maintain and update the recommended practices. Support organizations adopting the practices administratively and technologically.
Responsibility: Private sector consortia
Anticipated Timeframe: Now and ongoing

**7. Non-Covered Entities**

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.
Activities: Develop and implement legislation to ensure that such entities maintain appropriate privacy and security practices. Work in partnership with the Oregon Attorney General, who is a voting member of the State e-Health Alliance, and the National Conference of Commissioners on Uniform State Laws.
Responsibility: State government, with private partners
Anticipated Timeframe: Special 60-day legislative session in 2008

**8. 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
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.
Activities: Identify different types of secondary use and development of 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.
Responsibility: State government, with private partners
Anticipated Timeframe: Next legislative session

**9. Enforcement**

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.

Activities: Evaluate applicability of current law to the HIE environment. Examine enforcement needs within the HIE environment. Create programs to fill those needs.
Responsibility: State government, with private partners
Anticipated Timeframe: Next legislative session

## Appendix B: Executive Summaries of Central Florida, Tennessee, & Rhode Island Focus Groups

**Rhode Island Health Information Exchange**
**Concept Testing and Positioning Research Report**
**May 2006. Magnet, Inc.**

Most participants have not been victims of malpractice or erroneous medical information, so they do not fully appreciate the pressing need for the HIE. Fortunately, medical mishaps are the exception rather than the rule for most people.

The HIE stands as one of those ideas that could be good if all security issues are handled.

The HIE is generally accepted, perhaps begrudgingly, as inevitable. As with the IRS e-filing system, most assume all records will eventually be automated. Emerging electronic medical systems such as United Healthcare's should help to set the stage for the HIE.

A gradual roll-out approach as opposed to all-in mandatory approach will make people more comfortable.

"Treating the whole person" (the underlying idea) should appeal to the broadest range of people. Most people are willing to believe and many have recently learned that seemingly unrelated medical issues can be connected. More caregivers' eyes on one's care is an appealing idea.

"It's like that ad for women and infants where doctors from everywhere are looking at the patient's cancer."

A strong public relations effort on the merits of looking at the big picture will heighten receptivity to this approach.

Saving lives is compelling for those who have had a medical scare. However, many people have been going through the healthcare system without any major problems, so this value proposition is not compelling for everybody.
Appealing on behalf of spouses, partners and children of the patient could be effective, particularly with spouses of older men who sometimes drag their feet when it comes to going to the doctor. In that vein, telling people to "get electronic" for their loved ones might be an effective approach.
Keep the emphasis on clinical outcomes even if there are efficiency benefits. Beware of efficiency claims since this sets up an expectation for lower costs.

Consider implementing the HIE through the physicians' practices and having them treat it more as an FYI with patients. Asking patients to consider enrolling exacerbates concerns. Then use more aggressive methods to pull in stragglers and hold-outs.

The best strategy is to start implementing the technology and talk about the benefits. The more people think about it without sufficient benefits explained, the more concerned they become.

**Central Florida Focus Group Reports**
**Perceptions among key stakeholders**
**June 2006**
**Health Council of East Central Florida, Inc.**

(Please see attached hard copy document)

**CareSpark survey (general public)**
**231 Total responses as of 10-10-06**
**Survey responses: 144 from Women's Health and Wellness Fair March 2006**
**14 from Scott County Rotary Club March 2006**
**11 from Clinch River Health Service April 2006**
**62 from Eastman Health Fair**

**1. What kinds of information would you be comfortable sharing among health professionals, for the purpose of coordinating and improving the delivery of health care services to you?**
*216 (93.5%)* name, address, phone, date of birth
*61 (26.4%)* social security number
*112 (48.4%)* payment information (health plan, health savings account, credit card, or other)
*140 (60.6%)* employer
*206 (89%)* past history for health issues (childhood, previous illness or injury)
*209 (90.4%)* list of current medications, including vitamins, over the counter medications and herbal supplements
*195 (84.5%)* allergies
*195 (84.4%)* names of physicians or other health professionals from whom you receive care
*173 (74.9%)* preferred choices for pharmacy, lab, diagnostic services, inpatient services
*126 (54.5%)* mental health diagnosis / treatment history
*116 (50.2%)* sexually-related diagnosis / treatment history
*126 (54.5%)* infectious disease history (HIV, tuberculosis, hepatitis)
*152 (65.8%)* chronic disease conditions (diabetes, lung disease, cancers)
*171 (74%)* family history of disease
*3 (1.3%)* none
____ other (please explain)

**2. What methods would you use to give permission?**
*156 (92.3%)* sign paper form at doctor's office, hospital, pharmacy, lab, clinic, etc.
*32 (18.9%)* sign paper form at other location (mall kiosk, etc.)
*27 (16%)* sign-up online

**3. To whom would you give permission to view your information?**
*214 (92.6%)* to doctors who are responsible for my personal health care services
*172 (74.4%)* to nurses or other office staff who assist my doctors
*161 (69.6%)* to my pharmacist
*107 (46.3%)* to technicians in laboratories, imaging centers, clinics
*162 (70%)* to emergency responders (EMS, ambulance, etc.)
*115 (49.7%)* to home health agencies, caregivers
*77 (33%)* to public health officials responsible for tracking bio-terrorism, disease outbreaks, public health trends
*67 (29%)* to organizations conducting research for clinical purposes (medical treatment procedures, pharmaceutical, medical devices, etc.)
*57 (24.6%)* to persons tracking and reporting quality improvement measures
*57 (24.6%)* to persons tracking and reporting cost-efficiency measures
*104 (45%)* to those responsible for payment for my health care (employer, health plan)
*168 (72.7%)* to family members who would make decisions if I am incapacitated

**4. What kinds of information in your records would you expect to have access to view?**
*180 (77.9%)* list of all who have viewed my records (stamped with time and date of access, list of information viewed)
*189 (81.8%)* all information in my records
*34 (14.7%)* some information in my records (explain what this might include):

**5. Who is responsible for protecting the security of my information?**
*182 (78.7%)* I am
*198 (85.7%)* my health care provider
*85 (36.7%)* CareSpark staff who are employed to maintain system security
*47 (20.3%)* CareSpark board of directors
*82 (35.4%)* state / federal government

**6. What should be the penalties for release of information without permission?**
*85 (36.7%)* reprimand, retraining of employee
*96 (41.5%)* firing of employee
*121 (52.3%)* loss of certification, license or credentials for health professional
*78 (33.7%)* loss of business license for organization
*89 (38.5%)* civil charges, fines
*39 (16.9%)* criminal charges, time in jail
*7 (3%)* other (please specify): *depends on the severity, intentional or not*

**7. How would we best communicate with you about the system?**

*119 (51.5%)* verbal explanation at health professional's facility
*115 (49.8%)* written explanation at health professional's facility
*62 (26.8%)* online website for information
*45 (19.4%)* general media information
*79 (34.2%)* direct mail from your health provider
*11 (4.8%)* other (please specify)

**8. What benefits do you perceive from the electronic exchange of health information?**

• Information when you need it
• Communication is an issue if doctor uses paper charts
• Ease in changing primary care, advice of specialty
• All have same information
• Convenience
• Technology error
• Human error
• Reduced duplication
• Faster service for patient
• fewer mistakes
• Helps make things better for all who work in the medical field, access to more patient info
• Improved continuity of care, better coordination
• Lessen multi-doctor, poly-pharmacy syndrome
• A lot less paperwork, time spent finding charts
• More accurate
• Remote access for clinicians
• Faster response time for lab, x-ray results
• Access to information about new treatment options
• Better diagnosis, treatment
• Accuracy at pharmacy
• Avoid conflicts in medication, errors
• Saves time in emergency situation
• Reduced duplication
• Cost control
• none

**9. What risks do you perceive from the electronic exchange of health information?**

a. Too many persons have access
b. Privacy and confidentiality is at risk
c. Pharmaceutical companies could use info
d. Inaccurate information available in situations where it is not needed (not life-threatening)
e. Technical error
f. Human error
g. Mistakes (such as when people have the same last name)
h. Misuse of information

i. Missing information
j. Something could be deleted with no way to recover records
k. Problems with .down time.
l. Insurance company will increase rates
m. Inaccurate information could result in wrong treatment
n. Family or personal history of disease could impact employability
o. None
p. Sale of data to vendors
q. Identity theft

Markle, findings about trust of MDs, Health plans, corporations <Jody Slides>.

## Appendix C: RAND Study on Patient Identifiers (HIMSS 2007)

Rideout, J and Hillestad R (2007). The RAND study on Patient Identifiers. HIMSS07 Annual Conference and Exhibition. Education Session Number: 58. http://www.himss07.org/education/viewsFromTop.aspx. Accessed 3/14/2007.

**Description**

Patient identity establishment is the process by which an individual is unambiguously linked to his/her healthcare information. Unequivocally establishing this linkage is a fundamental requirement for meaningful health information technology interoperability. Recently, RAND has been performing an in-depth analysis of the key technical, social, political, legal and economic factors involved in developing a system for establishing patient identity, within the architecture of a National Health Information Network (NHIN), and for utilizing that system to access authorized health information from multiple and disparate electronic record sources while preserving patient privacy.

**Slide Summaries**

**Health Care Identity**

Health care identity is the quality of being a unique person. It links a person to their health information. An *Identifier* is a symbol, pattern, or collection of attributes that denote a unique healthcare identity. *Identification* is the process of establishing which healthcare identity belongs to a specific person. It consists of claiming to own the identity plus authentication. *Registration* is the process by which a patient obtains or establishes a link to their healthcare identity.

**Why is Healthcare Identity a Problem?**

Most current identity systems cannot link across organizations. Interoperability of health systems requires a common approach to identity, authentication, and linking patients to their data. Security and privacy concerns, political, and financial barriers limit the range of acceptable identity solutions in healthcare. These barriers slow development and limit the benefits of interoperable healthcare IT.

There is a tension between linking health information and privacy of the individual. The risks of health care identity solutions must be balanced against the costs and potential benefits.

**Healthcare identifiers in the United States**

A universal national healthcare identifier was legislated OUT of HIPAA. There has been no progress on a national identity standard in healthcare. Most RHIOs use a probabilistic/algorithmic identity process to link patients to their health information. There is a strong need to create a standard for patient identity and authentication in the US.

**Potential Benefits of Healthcare Identity**

The benefits of healthcare identity go beyond immediate health care. A standard approach would enable improved health quality, safety, and efficiency. There would be better opportunities to use health data for research, Public Health, disaster response, and healthcare system transformation.

**The RAND Patient identity Establishment Project**
The RAND study aims to identify and assess the issues around healthcare identity, identify candidate solutions, and assess those solutions for technical performance, privacy and security, impact on patient choice, policy implications, and cost as it relates to real value.

**Environmental Scan Summary**
The public is worried about releasing personal health information and widespread adoption of healthcare IT can increase the risk of undesirable disclosure. Consumer advocates strongly resist adopting a universal unique identifier in healthcare. Concerns about privacy and security are difficult to separate from the identity process itself. Today's RHIOs and HIEs are all using algorithmic identity processes, rather than unique identifiers for patients. Legal concerns persist about federal privacy rules and state laws, including variances between states. Other countries use unique healthcare identifiers, but they are different from the US.

**Other Countries Differ from the US**
Most countries that use universal unique identifiers in healthcare require universal participation. They are more likely to have national privacy commissions and strong enforcement of privacy rights. The consequences of exposure are less for insurability and employment.

**4 Models for Linking Patients**

- Universal Identifier
- Algorithmic matching
- Personal Health Record
- Public Key Encryption

**3 Dimensions of Analysis**

- Cost
- Technical merits
- Value added

**Cost Estimates**
To create a new method of establishing healthcare identity would result in a one-time cost of between $3 and $30 billion plus renewal costs.

**Technical Analysis**
RAND created a reference architecture, and developed use cases to test possible solutions.

## Value Analysis

### Key Issues for Universal Identifiers

Does a Universal Identifier add significant value over other approaches? What other value does it add for health quality, safety, and efficiency, research, Public Health, disaster response, and healthcare system transformation? How can we overcome the problems with universal identifiers? What are the governance and policy implications? What are the real costs? Is there a voluntary approach that would get significant uptake?

### Key Issues for Algorithmic Methods of Healthcare Identification

How well does it scale to the region/nation? What constraints does it place on architecture? How could it be combined with a voluntary identification number? What are the total costs? What are the privacy and security issues? How does it facilitate patient control of access and compartmentalization?

### Key Issues for Personal Health Records

What role does the PHR play in NHIN? What are the privacy and security implications?

### Key Issues for Public Key Encryption

What role does PKE play in NHIN? How does it facilitate patient control of access and compartmentalization? Will it get in the way of an effective solution? Can it coexist with other approaches? What are the privacy and security risks? What will it cost?

### Conclusions

The current situation in healthcare information management provides security through obscurity. Greater sharing of health data entails greater security and privacy risks. Potential misuse of widespread electronic health information makes privacy and security a crucial component of a solution. Decisions about approaches for linking patients should be based on solid data.

## Appendix D – Background, Sources, Related Documents

The MPHIE Mobilization Planning effort was commissioned and financed by the Oregon Business Council's Health Information Exchange Leadership Group. The project leadership team (Tiger Team) provided oversight and leadership in guiding the development of the planning included:

Andrew Davidson, Oregon Association of Hospital and Health Systems
Janice Forrester, PhD, The Regence Group
Dick Gibson, MD, PhD, MBA Providence Health Systems & Legacy Health Systems
Jody Pettit, MD, Oregon Health Care Quality Corporation & Office for Oregon Health Policy and Research

The Mobilization Planning effort was staffed by Oregon Health Care Quality Corporation. Staff and sub-contractors who contributed to various portions of this report include:

Nancy Clarke
Jody Pettit, MD
Tom Ricciardi, PhD
David Witter, Witter & Associates

For More Information please contact:

Oregon Business Council
1100 SW 6th Avenue, Suite 1508
Portland, OR 97204
Denise Honzel, honzelde@aol.com,
(503) 860-1278

Oregon Healthcare Quality Corporation
619 SW 11th Avenue, Suite 221
Portland, Oregon 97205
Nancy Clarke, nancy.clarke@q-corp.org
(503) 241-3571

The Mobilization Planning effort builds upon the report to the Oregon Business Council (OBC) Data Exchange Group titled "Oregon Health Information Exchange Options" dated May 15, 2006 available at http://www.q-corp.org/q-corp/images/public/pdfs/OR%20HIE%20Options.pdf.

The Mobilization Planning effort report relies on a number of sources of information including published studies, publications and reports of major organizations involved in health information exchange, and information collected from other regional health

information organizations (RHIOs) and health information exchanges (HIEs) and interviews and discussion with clinicians and other stakeholders in the community.

Key Mobilization Planning documents include

- MPHIE Final Report
- Metropolitan Portland Area Health Care Environment.
- MPHIE Technology Plan.
- MPHIE Privacy and Security Assessment.
- MPHIE Governance Plan.
- MPHIE Business Plan.
- MPHIE Operations Plan.