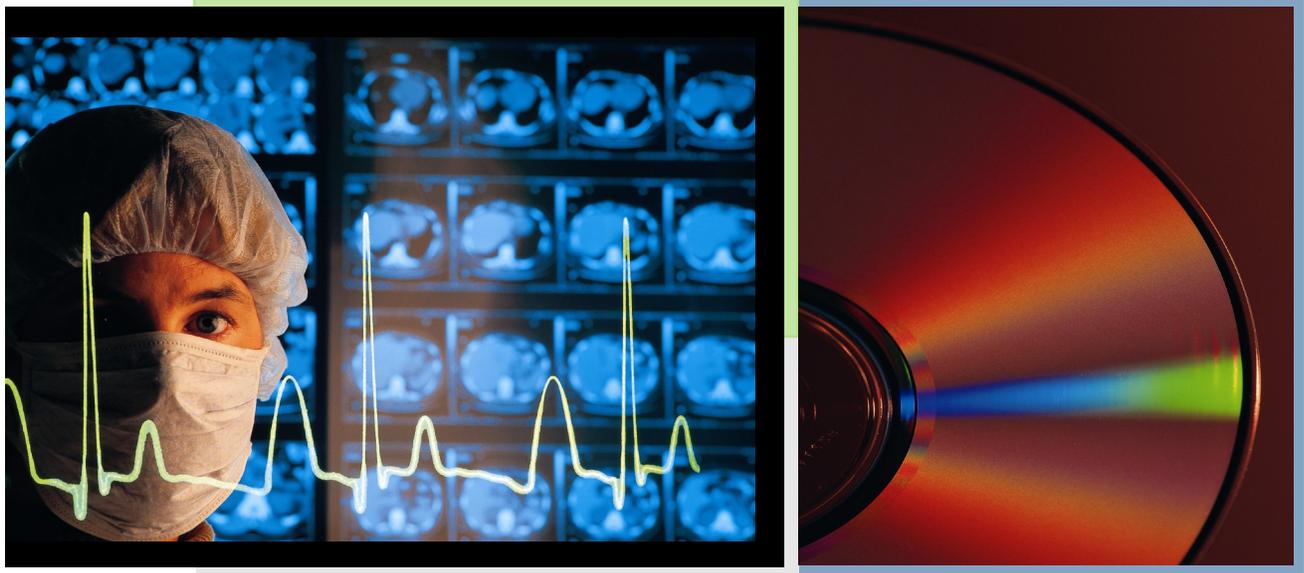


Interoperable Solutions for Health Information Exchange:

An interim summary of solutions to advance eHealth in Utah.

January 2007



Utah Network for Electronic Public Health Information- Privacy and Security

Submitted by: Lois Haggard, Ph.D, Project Director
Utah Department of Health
P.O. Box 142101
Salt Lake City, UT 84111-2101

Submitted to: Cynthia Irvin, Ph.D., State Liaison
Research Triangle Institute
P.O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC
Contract No. 290-05-0015



A Utah Department of Health report for the
Health Information Security and Privacy Collaboration (HISPC), January 2007.

The Utah Department of Health Utah Network for Electronic Public Health Information Privacy and Security (Unify-PS) Project expresses its gratitude for the assistance, time and effort of the individuals and organizations that participated in the Project Work Groups and survey process. Participants' voluntary time and input has been critical to identifying and documenting the privacy and security concerns in health information exchange and accomplishing the project objectives.

This project is funded through a grant from the Research Triangle Institute.
Contract no. 290-05-0015

Questions or comments regarding this report should be directed to:

Francesca Garcia Lanier, Project Coordinator
Utah Unify-PS
Utah Department of Health
348 East 4500 South
Salt Lake City, UT 84107

Email: flanier@utah.gov
Telephone: 801.892.6649

Table of Contents

- Background 1
 - Purpose and Scope 1
 - Utah eHealth 1
 - Limitations 2

- Assessment of Variation 3
 - Main Findings 3
 - Effective Practices 4
 - Lessons Learned 5

- State Solutions Group 5
 - Stakeholders 5
 - Work Group Process 5

- Proposed Solutions 6
 - Technical 6
 - Administrative 12
 - Education 15
 - Legislative 16

- Attachments 17
 - A. Decision tree 17

- References 18

1. BACKGROUND

PURPOSE & SCOPE



The purpose of this report is to document privacy and security solutions identified by the Solutions Work Group (SWG). Proposed solutions address barriers to health information exchange that result from variation in organizational-level business practices, policies, and regulations that underlie such practices. The SWG reviewed the business practices for exchanging health information reported in the Interim Assessment of Variation Report, November 2006. The business practices were classified by the Variations Work Group (VWG) as presenting a barrier to the secure and private electronic exchange of information. Business practices were subsequently reviewed by the Legal Work Group (LWG) to identify federal or state statutes that explain why the reported practice is in place. The solutions presented in this document are intended to preserve essential privacy and security protections while moving forward electronic connectivity to permit appropriate exchange of health information.

UTAH eHEALTH

Utah's healthcare system, along with that of the nation, is moving into the electronic age. The secure sharing of health information electronically is referred to as eHealth, and it is making great strides in Utah to improve how doctors, hospitals, health insurance companies and public health departments are meeting the healthcare needs of all Utahans.

Patients in rural areas of the state benefit from telehealth (the use of electronic information and telecommunications technologies to support long-distance clinical health care and patient education) opportunities that electronic medical records can provide.

Quality of patient care is expected to increase when physicians have more complete information on a patient and can provide better continuity of care. For example,

each day in Utah, doctors see nearly 2,000 patients in hospital emergency departments. Emergency department doctors need information on patient medications, allergies and disease history. Getting the information from a patient's doctor quickly and efficiently would literally save lives in many cases.

The core technology to accomplish health information exchange is electronic medical records (EMR). The Utah Health Information Network (UHIN), which routes electronic insurance billing transactions for 95 percent of Utah health care providers, estimates that 20 percent of Utah physician offices have adopted EMR systems.

In a recent experiment conducted in Utah and Idaho¹, doctors were given hand-held personal digital assistants (PDAs) programmed with a decision-support tool. The doctors who used the PDAs were more likely to prescribe appropriate antibiotics and less likely to overprescribe them. Decision-support systems such as this can be built into an EMR system.

Much of the eHealth activity in Utah involves leveraging existing technologies and information standards that have been developed through community participation in UHIN. Specific projects are underway to provide electronic sharing of laboratory results from the lab to the doctor, hospital discharge notes from the hospital to the doctor, a patient's medical and medication history from one doctor to another, and e-prescribing.

So far, none of Utah's planned projects includes maintaining a central database of patient information. In all the Utah eHealth projects, the initial goal is to transform the paper transactions that are already happening or should be happening and make them more efficient and secure. The first step is somewhat similar to the difference between a fax and

“We are taking advantage of every opportunity available to promote eHealth in Utah,” said Dr. David N. Sundwall, UDOH executive director. “The health field needs to catch up when it comes to exchanging information electronically, and developing sound, uniform practices for preserving the privacy and security of health information is a prerequisite for moving eHealth forward.”

an email.

Although much of the activity in Utah and the United States involves the private healthcare community, Utah’s public health system can benefit from eHealth initiatives, too. The Utah Department of Health (UDOH) has begun a yearlong planning effort to develop a business plan for the public health system to participate in sharing of clinical information. The Utah Network for Electronic Public Health Information, or the UNIFY project, has the goal of evaluating the potential benefits of sharing information between the clinical care sector and the public health system. It is especially focused on surveillance of reportable diseases, vital records, newborn screening and immunizations.

Other active eHealth efforts of the UDOH include the Utah Patient Safety Program, Medicaid Management Information System, the Utah Immunization Registry, and the Child Health Advanced Record Management (CHARM) child health information integration program. In addition, the Utah Bureau of Epidemiology has a partnership with UHIN to expand the Real-time Outbreak Detection System (RODS), which was implemented during the 2002 Salt Lake City Winter Olympics to conduct disease surveillance in Utah’s emergency rooms and pharmacies.

handling requests for patient information (see scenario one - patient care A). Also serving as an impediment to the SWG process was a perception, on the part of solution work group members, that vested stakeholder interests in HIE ultimately may have resulted in a precautionary approach to providing solutions as multiple interests were involved and proposed solutions may be viewed as an infringement on livelihood or a critique of the business model.

LIMITATIONS

The SWG included members of the VWG with a determined and vested interest in the future of health information exchange (HIE) in the state of Utah. During the SWG process additional barriers were identified and information collected regarding inapplicability of scenarios to the state of Utah, and representativeness of the business practices to the state as a whole. For example, it was noted that a payer would not request access to medical charts (see scenario five - payment), and disagreement was noted between emergency room physicians for

2. ASSESSMENT OF VARIATION MAIN FINDINGS



The privacy and security concerns identified in the Assessment of Variation report were a mix of organizational, technological, educational, and legal issues. This was likely due to the nature of the scenarios used to collect the business practice data. For instance, stakeholders viewed some scenarios, or portions of the scenario, as atypical, unrealistic, or inappropriate. In addition, events that require the exchange of health information with agencies outside of the healthcare arena (e.g. law enforcement) were difficult to consider within the scope of interoperable health information exchange.

Authorization to disclose. Disclosing patient information without authorization is allowable under HIPAA for “treatment, payment and healthcare operations.” However, most providers choose to get patient authorization prior to disclosing health information. This did not appear to be an education issue, as providers generally understand this HIPAA provision and what constitutes an allowable disclosure. For many health care providers, the garnering of patient consent/authorization is an effort to ensure the patient’s right to privacy, minimize the provider’s risk of liability, or a practical procedure to aid the flow of information. In some cases, facilities refuse to release the patient information without patient authorization, even though it is allowed under HIPAA.

Transmission and transmission security of Protected Health Information (PHI). There is substantial variation in the means of transmission and security employed. On one hand, some physicians (in a physician office setting) reported regularly disclosing health information over the phone to other health care professionals once they had established a common level of understanding and trust with the requestor. On the other extreme, substance abuse providers have developed complex procedures for transmission that include:

verification, physical safeguards, warnings on paperwork about 42 CFR Part 2, and required acknowledgment receipts.

Long-term care facilities reported use of electronic facsimile (fax) as their method of choice for health information transmissions. Moreover, hospitals, physician offices, and other major stakeholders used fax regularly but also reported using mail, courier, and patient pickup. Selected large hospitals and integrated delivery systems have the ability to use encrypted email but this method is not yet widely used and accepted. Some facilities reported having policies in place that prohibit email use at all for transmission of patient information. In all but a few instances, fax continued to be the predominant method of transferring health information.

Electronic methods (CDs and the Internet) reportedly are employed with radiology films (e.g. x-rays), especially among large facilities. Mammography films are an exception. Some selected large facilities reported having the capability to make CD’s and use the Internet (by Picture Archiving and Communication System - PACS) to transfer mammography films, but rarely using these methods. Instead, films are typically transferred by in-person pickup with approved photo identification or sent by U.S. mail.

Applicability of relevant rules and statutes. Difficulty in exchanging health information increased when different rules and statutes apply to entities involved in the exchange of health information. Law enforcement is not a covered entity under HIPAA nor are Public Health or State Public Health Laboratories. Although substance treatment facilities are covered entities, they must also comply with 42 CFR Part 2, a federal regulation that heightens protections for treatment

records. Primary care providers often reported disregarding treatment facilities' records because the associated difficulties in accessing them. HIPAA and 42 CFR Part 2 do not align in a manner that is conducive to health information exchange.

EFFECTIVE PRACTICES

E-Health in Utah is quickly becoming accepted as a means to improve healthcare, lower costs, and promote healthier communities. It is clear that to continue to move eHealth forward towards an interoperable system that can communicate with other agencies and organizations while maintaining privacy and security, an open dialogue is needed to gain common understanding.

The SWG reassessed each business practice to determine whether the barrier the practice presented was appropriate and necessary to maintain privacy and security and to identify solutions to any challenge for moving to an electronic environment. Forty percent (n = 58) of the reviewed business practices were reclassified by the SWG as an aid, outnumbering those business practices that were classified as either barrier (n = 44) or neutral (n = 42). A decision tree process was used to assess each practice on degree to which privacy and security was maintained and capacity for an electronic exchange.

Business practices that sought patient authorization or consent to use or disclose health information were most commonly identified as an aid, regardless of whether the use/disclosure was allowable without patient authorization under HIPAA's treatment, payment or healthcare operations provision. The concern for privacy and security was mirrored by the SWG conversation that sought to repeal CFR 42 Part 2, not as a result of the law's stringent approach to the disclosure of substance abuse information, but because all personal health information is worthy of high standards for security, protection and equal treatment.

The SWG recognized the concern that certain types of information (such as that related to sexually transmitted diseases, mental health treatment, chronic disease, genetic testing results and substance abuse treatment) have a risk for misuse that could cause significant harm to the patient. However, such misuse is most likely to occur when the information is used and/or disclosed for purposes other than treatment. The SWG maintained that the benefit to patients outweighs the risk of harm when all relevant health information, regardless of type, is made easily available for treatment purposes.

It should also be noted that the SWG defined business practices detailing two entities entering into a business associates agreement, in all situations where data were shared, as an aid because it theoretically covers the entities not once, but twice. In addition, this practice, whether necessary under HIPAA, provides protection to both the entity and the consumer further illustrating the lengths to which providers, payers, etc. will go to prevent the misuse of health data as well as add legal protections.

Information can and should carry inherent protections but the benefit of accessible personal health information for quality care is to the patient. Utah laws exist to provide protections for other sensitive health information. Those laws do not place restrictions on using the information for legitimate treatment purposes. Examples of Utah laws that specifically address disclosure of sensitive health information include the Mental Health Professional Practice Act (UC 58-60-114) and Genetic Testing Privacy Act (UC 26-45).

LESSONS LEARNED

The value stakeholders place on privacy and security is at a premium. Solutions Work Group resonated with the Assessment of Variation finding that providers seek patient authorization to release patient information even in instances where authorization for such a release is not required (treatment, payment, and healthcare operations purposes) further classifying the practice as good practice. This theme held true throughout the Solutions Work Group efforts as the group reclassified many business practices from barrier to aid because the practice was viewed as providing the consumer with a higher degree of privacy and security. Many practices were appropriate and necessary measures that serve as a check and balance to protect an individual's privacy and security.

3. STATE SOLUTIONS

STAKEHOLDERS



Members of the SWG were selected from a representative group of healthcare community professionals interested in health information exchange (HIE) in the state of Utah. Linn Baker, Director for Utah's Public Employee Health Program and board member of the Utah Health Information Network, the state's largest regional health information organization (RHIO), chaired the SWG. Additional group members included two emergency room physicians (one of whom participated in the VWG and has just recently completed his MS in medical informatics), a compliance consultant at an integrated delivery system (who also served on the VWG), a detective for a small suburban area north of Salt Lake City (who also served on the VWG), the assistant director of the RHIO for the state of Utah (who also served on the VWG), the CEO of a home healthcare agency and hospice, the legal consultant for the largest payer in the state of Utah, two employees of the Utah Department of Health, and a faculty member of the De-

partment of Medical Informatics at the University of Utah.

SWG PROCESS

The stakeholders involved in the SWG met on five separate occasions for two hours time to review business practices and determine which business practices constituted an appropriate barrier to the electronic exchange of health information.

The initial meeting revealed the need to reclassify business practices as an aid, neutral or barrier with regard to electronic exchange and consumer privacy and security. SWG members used a decision tree process to assess whether business practices pose a barrier to electronic exchange and privacy and security (See Attachment A).

The SWG members were assigned the task of identifying solutions to the business practices identified as barriers to the electronic exchange of health information in a secure and private environment. SWG members were assigned business practices based upon expertise and experience and tasked with identifying potential solutions using guided criteria. Members provided their findings during the SWG meetings. A minimum of two SWG members were assigned to present a solution at each meeting. Input was solicited from the respective SWG member(s) at the facilitated SWG meetings.

Business practices were organized into four broad categories in need of solutions: technical, administrative, education, and legislative. Solutions for each category are presented in the following section. Current and planned electronic projects were incorporated into solution results where possible and appropriate. The following solutions represent the SWG ef-

fort to address identified challenges to the electronic exchange of health information while maintaining the security and privacy of that information. They are not intended as a definitive statement but rather to provide a framework for further dialogue regarding appropriate information exchange in a secure and private environment.

4. PROPOSED SOLUTIONS

TECHNICAL



Challenge - *Accessing appropriate information.*

Solution. Establish a Utah payer-based member identifier that is unique and recognizable across all participating payers. This voluntary system would start within the payer community with healthcare entities ultimately having the option to adopt this unique member identifier.

General context. The unique patient identifier has not been defined in Utah due in part to privacy concerns and because there is as of yet no law protecting the individuals privacy beyond that of HIPAA. Further, the need to coordinate multiple agencies (HHS, Medicare, CDC) and systems is necessary to move forward with a single identifier at the federal level.

Privacy and security domain. All.

Types of HIE. Administrative in the short-term; clinical in the long-term.

Stakeholders primarily affected. Payers, providers, consumers.

HIE barriers addressed. All.

Stage of development. Functional assessment.

Extent to which solution is in use. Policies are in place for limited sharing only. However, no common identifier exists.

Applicability of solution. Applicable across industry. Standard identification of member data. Unique member identifier is a key requirement for expediting electronic exchange.

Extent of barriers or opposition. Cultural barrier, competition, clarifying the value proposition, funding.

Challenge - *Lack of search capability.*

Solution. Establish a structure to assist in locating the patient-specific health information contents. This can include a record locator, patient record bank, or other type of central patient repository.

General context. Advances in IT have made possible the ability to bridge disparate applications and languages. As information needs change and grow in scope and complexity the enormous value IT brings is in its ability to link and merge health information.

Privacy and security domain. All.

Types of HIE. Clinical, administrative.

Stakeholders primarily affected. Providers, consumers, payers.

HIE barriers addressed. All.

Stage of development. Planning.

Extent to which solution is in use. UHIN is piloting clinical data exchange and developing methods to “push” information out electronically but there is currently no mechanism to “pull” information in a timely manner. Private industry is developing consumer-driven health data banks.

Applicability of solution. Applicable across industry.

Extent of barriers or opposition. Privacy and security concerns with storing patient data in repository. Ownership of records is at issue, as is trust for industry held and consumer controlled data bank. Electronically searching multiple providers requires search capability and server reliability.

Challenge - *Limited ability to transfer/transmit PHI electronically.*

Solution. Establish an electronic 'pipeline' to all areas of the state.

General context. Rural health care facilities have relationships with distant healthcare providers with which they need to exchange information. Many rural areas of the state have limited infrastructure to support high speed networks. The Utah Telehealth Network has worked closely with telecommunications companies, the University of Utah, and the state of Utah to bring services to rural health care facilities with the development of the physical infrastructure to allow for connectivity.

UHIN's Web portal technology connects participating members to allow for the exchange of administrative information. In 2004 UHIN became an Agency for Healthcare Research and Quality (AHRQ) State and Regional Demonstration grant recipient. UHIN has expanded its focus to include the exchange of clinical healthcare data and is developing clinically-focused healthcare transaction standards.

Privacy and security domain. All.

Types of HIE. Clinical, administrative.

Stakeholders primarily affected. Providers, consumers, payers.

HIE barriers addressed. All.

Stage of development. Functional assessment.

Extent to which solution is in use. The Utah Telehealth Network links patients to health care providers across the state, country and world by using the most current telecommunications technology. Telehealth provides rural patients and providers with access to services that are usually available only in more populated urban areas. The Utah Telehealth Network uses interactive video to deliver patient care, provide continuing education to health professionals, facilitate administrative meetings, enable digital images such as CAT scans and X-rays to be transmitted for second opinions, and allows for emergency stroke patients to receive state-of-the-art stroke care during the critical three-hour window of treatment despite being hundreds of miles away from the nearest neurologist (see Figure 1).

UHIN's members include 100% of Utah's long-term care facilities and hospitals, 95% of physicians, one third of dentists, some laboratories and 450 payers.

Applicability of solution. Applicable across industry.

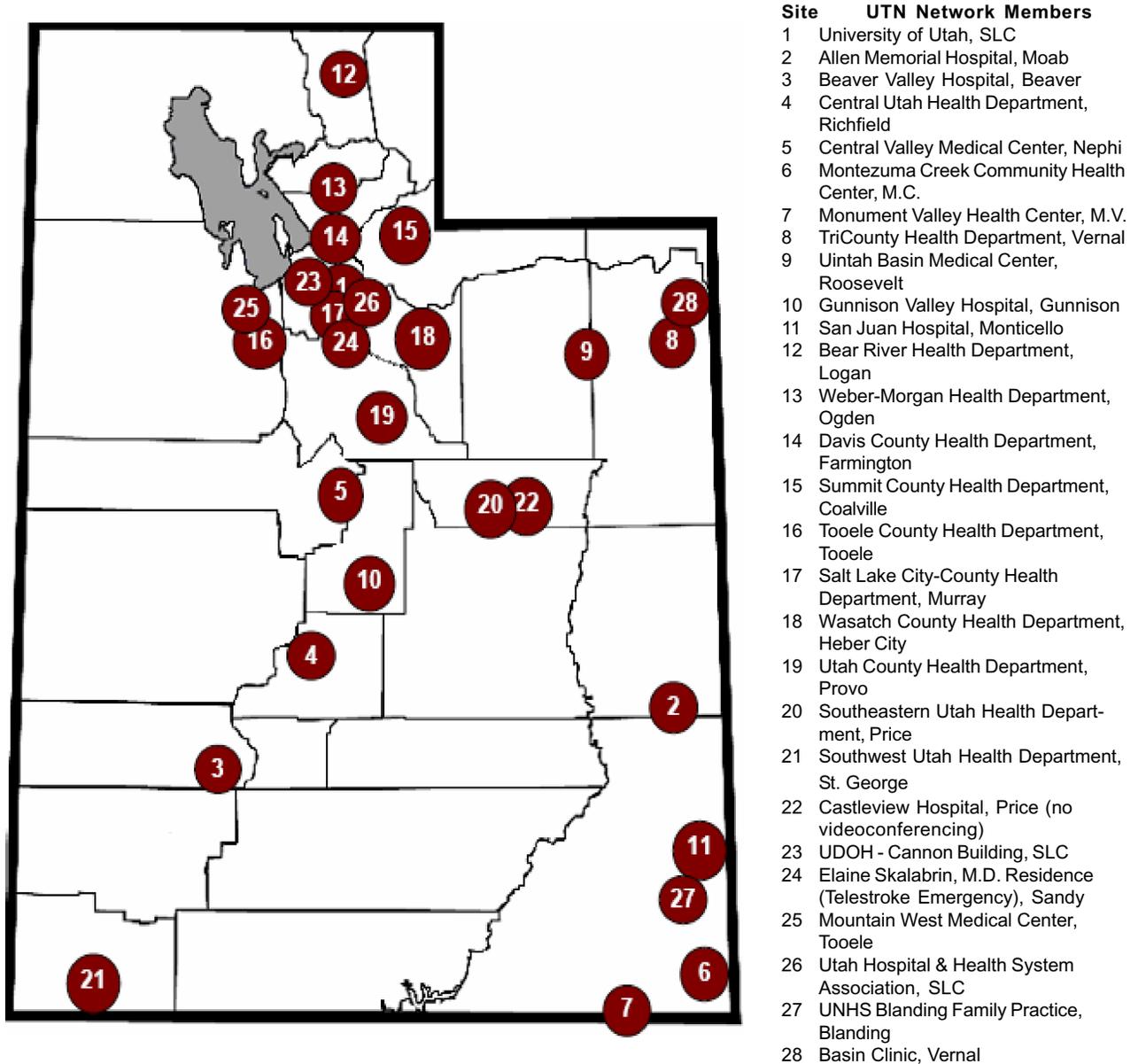
Extent of barriers or opposition. Political will, funding.

Challenge - *Authentication/ verification of physicians and providers.*

Solution. Establish system or standard protocol for authentication and verification of provider authority to access PHI.

General context. Authentication is essential to prevent the inadvertent or inappropriate release of information. All information should be accessible only on a need-to-know basis. Ensuring that information is only released after the identity of the requestor is confirmed is critical. Current security policies typically rely on a request faxed on letterhead.

Figure 1. Utah Telehealth Network Map of Sites



Source: Utah Telehealth Network, www.utah.telehealth.net
 Map date 12/2006.

Privacy and security domain. All.

Types of HIE. Clinical, administrative.

Stakeholders primarily affected. Providers, consumers, payers.

HIE barriers addressed. All.

Stage of development. Implementation & planning.

Extent to which solution is in use. UHIN currently visits each participating member to authenticate the member location and designate a site specific role manager. The role manager is responsible for verifying physicians and providers at their location.

Applicability of solution. Applicable across industry.

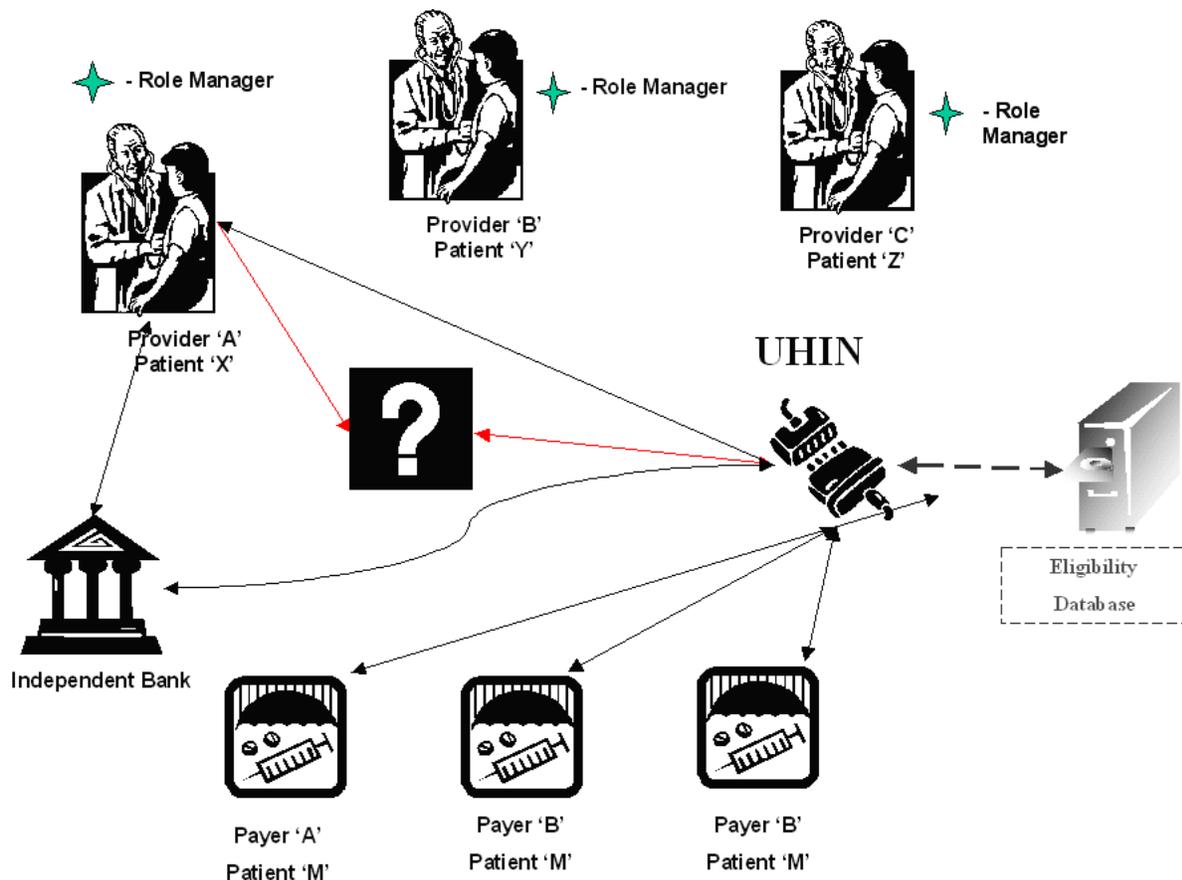
Extent of barriers or opposition. Community commitment to standards, funding.

INTEROPERABLE HIE

Short-term Model

The following model was proposed as a short-term state-wide solution to address the technical challenges to the secure and private electronic exchange of health information. The goal: to move Utah to-

Figure 2. Short-term Technical Solution



wards a single healthcare identifier for all Utah citizens. Step one involves Utah payers voluntarily adopting a single numbering system known in this document as the “common identifier.” The common identifier is a member identification number using a numbering standard set by the UHIN community standard-setting process. UHIN would host the numbering system database and would designate blocks of numbers to each payer voluntarily participating in the process. Assigning a common identifier to all participating payer members will be challenging. One consideration is identifying people with multiple coverage’s under different insurance companies to avoid giving them two numbers. A query system may be needed to identify those person that already have an assigned number. A longer term option may be to create a master patient index functionality. For the short term, the community wants to explore other options first.

All messages carried by UHIN are appropriately encrypted when in transit. UHIN is certified through the Electronic Healthcare Network Accreditation Commission (EHNAC) and employs reasonable and appropriate security and privacy practices.

Payers may choose to crosswalk their own internal member identification number(s) to the new common identifier or replace their proprietary member identification number with the new common identifier number.

Figure 2 shows the possible process for a request from provider ‘A’ for medical information on patient ‘X’ sent to a participating payer via UHIN using the common member identifier “M”. This process assumes that payers have adapted their claims information databases to be able to respond to queries for information about a specific member.

In the short-term model, providers would have already received the common identifier “M” for all members of participating payers and would have recorded that information in their practice management systems (the “M” identifier would also be used for billing purposes).

The UHIN community would come together to create standard messages for both the request for the information (from the provider) and the response (from the payer).

The provider making the information request would send the standard request message to the payer via UHIN. The payer would then locate the information on that member and respond with the standard response message containing whatever information they had available on that member.

This short term solution assumes that some of the other listed challenges have been addressed: that all health care entities are connected to this pipeline and that physicians and providers have been authenticated through the UHIN member authentication process. The short-term solution will be evaluated for the value it brings to the community so that it can be determined if it is an economically sustainable option.

Long-Term Model

Public and private entities around the state are moving toward electronic health information exchange and together are working to improve sharing medical data to enhance quality care. Security and privacy are of critical importance for all stakeholders and consideration must be given to the location, accessibility and ownership of medical records. Most providers and public health programs maintain their own patient records and are often hesitant to release them outside of their domain. A data-sharing orienta-

tion must be fostered to achieve a connected community where health information is exchanged in a secure and private environment.

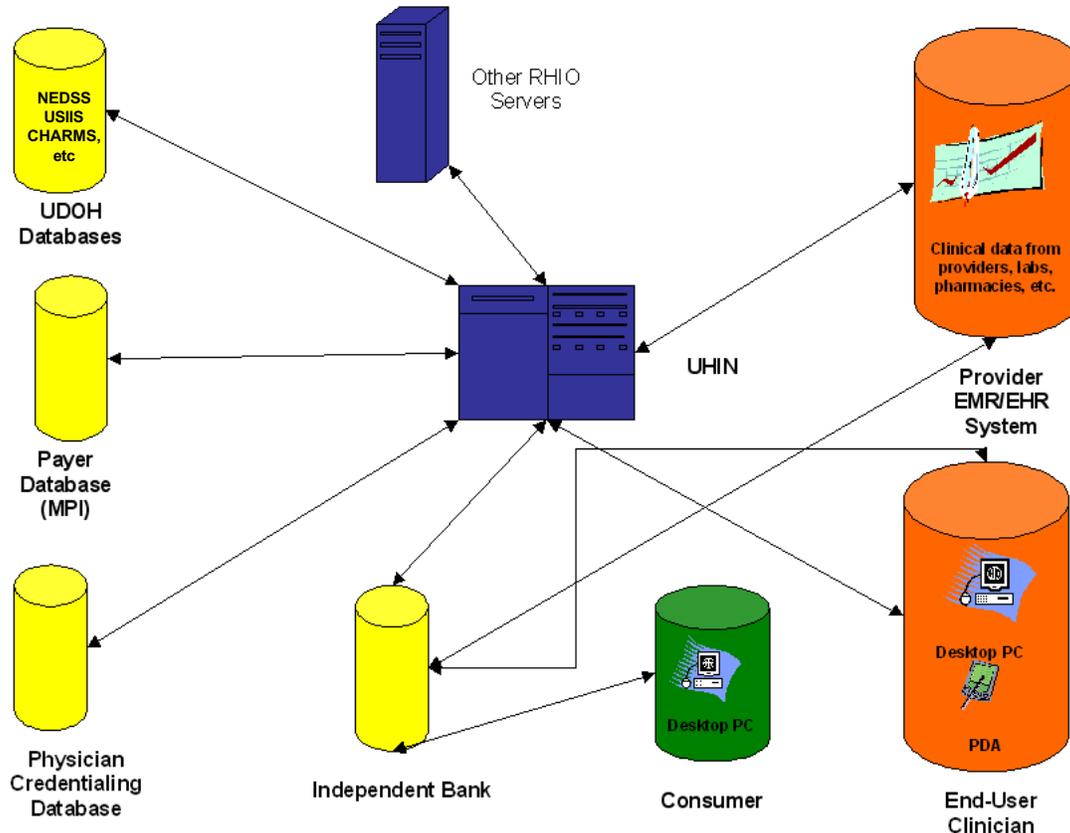
The high priority for privacy and security led SWG toward models that employ decentralized data-sharing arrangements or federated models of data location. In a decentralized or federated model, the data reside in the provider system and are accessed directly from the provider's or individual program (public health) database.

In the long-term solution, an assumption has been made that many Utah providers would have voluntarily adopted the common member identification number promulgated by the payers in the short-term solution. The value for providers is that it would assist them in de-duplicating their own records as well as make it easier to ex-

change information with other entities with some surety that the information being exchanged was truly about the correct person. In this way, it is hoped that the 'member' identifier would move to become more of a 'patient' identifier. We would have to determine how to assign uninsured persons an identifier. It is likely that this will require the adoption of a full-blown master person index functionality by UHIN but that decision would be made when the need warranted.

Data can be accessed in several ways (see Figure 3). Using the UHIN network among providers, each provider could contact other providers to request the appropriate records using the common identifier, and then receive those records from the source location. The UHIN network would maintain a database of patient common identifiers ("M") for every

Figure 3. Long-term Technical Solution



patient in Utah who has a medical record held in one of the databases connected to UHIN. UHIN would monitor the claim traffic already going through the network to create a record of where patients have been seen by health care providers. This functionality would have to be constructed to be compliant with both CFR 42 and with patient's consent to participate in the system.

When a patient record request comes to UHIN's server, UHIN will use the common identifier to point to information sources about the patient. UHIN will send the request to the information source(s), retrieve any information from the source and return the information to the requesting member. If a patient is not found, UHIN will inform the requesting entity of this. The ability to authenticate providers will be a strong asset in maintaining network security. Additionally, individual providers, if they know the information source (such as when a PCP has referred a patient to a specialist) could request the needed information from the information source by sending a request message directly to that source via UHIN without going through the UHIN search process.

In addition, it is envisioned that using payers as a source of information about patients (as described in the Short Term solution) would continue as an option.

The UHIN RHIO is a critical partner in the development of the infrastructure. Statewide connectivity is dependent on public/private partnership.

The long-term model is envisioned as a statewide health information infrastructure that enables healthcare professionals to access a patient's medical records from any provider or payer database connected to the network over a secure Internet connection. The public private effort transitions from the short-term and proposes to connect healthcare providers and public health across Utah. The long-term solution will be evalu-

ated for the value it brings to the community so that it can be determined if it is an economically sustainable option.

ADMINISTRATIVE

Challenge. *Intra-agency sharing of health information.*

Solution. Integrate state public health data systems to 1) facilitate the monitoring of the health of communities, 2) assist in ongoing analysis of trends and detection of emerging threats, and 3) provide information for setting public health policy. Work together to breakdown cultural barriers and facilitate the sharing of data across programs by establishing practical administrative procedures for information sharing between state programs (see Figure 4).

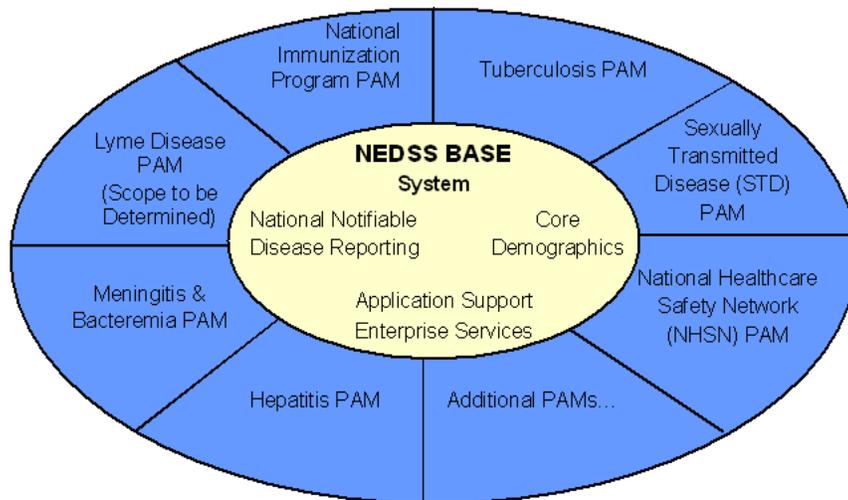
General context. The data systems that support the state health department lack a holistic perspective of the client. Data systems are singular information silos supported by categorical funding streams. Data cannot be easily exchanged, linked or merged by personnel from different programs. Program managers see their program data as a resource that they should maintain a high level of control over for the long-term benefit of their clients and the program itself. Program managers express multiple concerns about data sharing including misleading or misinterpretation of data, trust and organizational transparency.

Privacy and security domain. All.

Types of HIE. Public health, clinical.

Stakeholders primarily affected. State agency, consumers.

Figure 4. Conceptual Picture of NEDSS Base System and Program Modules



HIE barriers addressed. Intra-agency sharing.

Stage of development. Planning.

Extent to which solution is in use. Policies are in place for limited sharing only. A system similar to Figure 4 is in the planning stages. Separate data sets will remain independent while a central reporting database will communicate with all data sets and flag instances where health information overlaps. This will eliminate the need for multiple systems that have little or no communication capability and improve the delivery of services to program recipients. However existing cultural barriers make the sharing of any PHI among programs taboo.

Applicability of solution. Assist in rapid response to events that have the potential to develop into a major public health event. Programs can share data and find new ways to coordinate activities for improved services (weed out duplicative efforts, fill service

gaps).

Extent of barriers or opposition. The risk of providing general access to data may expose the data to accidental modification or deletion, breach of confidentiality, or misinterpretation. There is a real associated cost to sharing data. In addition, categorical funding streams limit or prohibit the sharing of data across programs.

Challenge - Information sharing with first responders.

Solution. Establish general protocols for first responders and what information can be shared when given responding situations.

General context. Improvements in communication and network development is an ongoing process. Public health, EMS, and law enforcement can continue to build relationships to work

together to develop processes to meet the information needs.

Privacy and security domain. All.

Types of HIE. Law enforcement, public health.

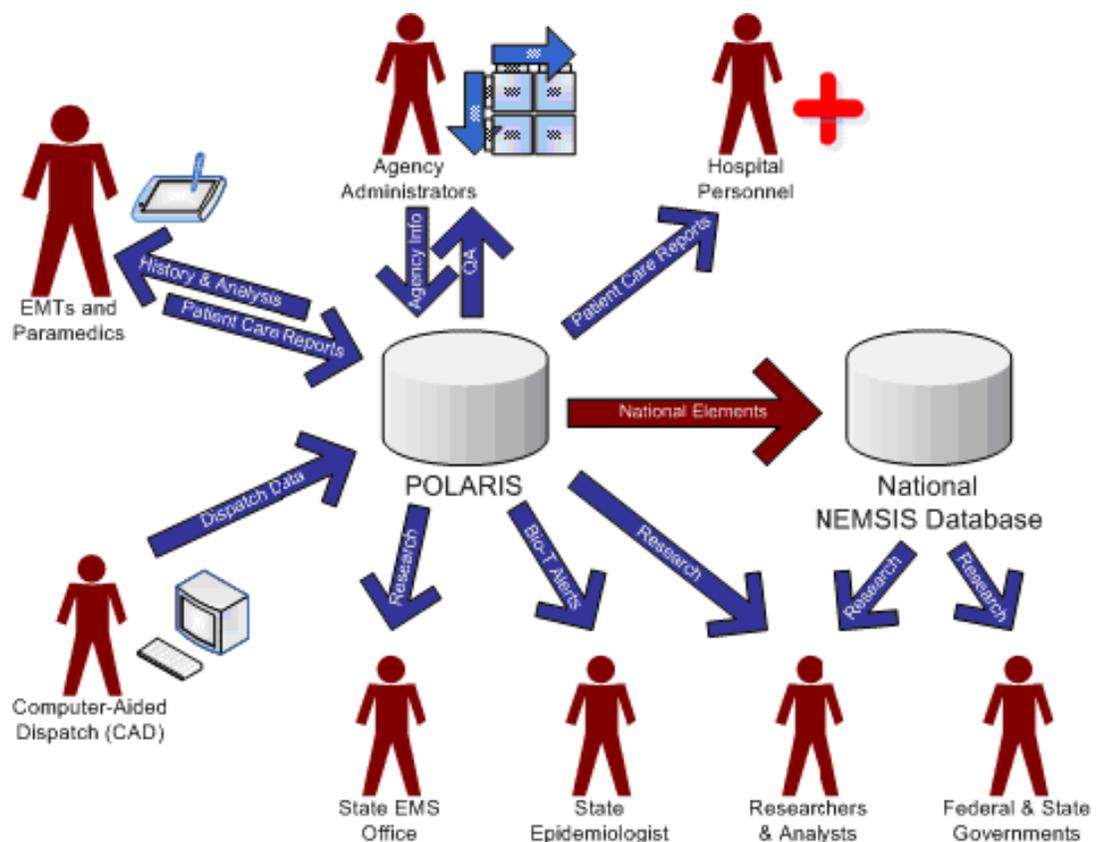
Stakeholders primarily affected. State agency, providers, consumers.

HIE barriers addressed. Intra-agency sharing.

Stage of development. Planning, implementation.

Extent to which solution is in use. First responders maintain a cohesive positive relationship in Utah. Emergency medical services are housed within the State Department of Health and police, fire and EMT are equipped with the National EMS information System (NEMSIS) that allows for local and national reporting of emergency data (see Figure 5). NEMSIS along with the Pre-Hospital On-line Ac-

Figure 5. NEMSIS/POLARIS



tive Reporting System (POLARIS) serve as Utah's first responder data system.

Applicability of solution. Communications system for first responders very relevant to connectivity and establishing practical relationships that allow for the sharing of necessary information with approved protocols.

Extent of barriers or opposition. Multi-agency coordination and commitment to joint training effort.

EDUCATION

Challenge - *Consumer misinformation regarding HIPAA and the use of personal health information.*

Solution. Increase consumer awareness of the benefits to accessible health information.

General Context. Consumer information comes from various media outlets including popular television shows. News media highlights the terrifying tales of security breaches. Little information is shared with the consumer regarding the benefits of having available and accessible ones personal health information.

Privacy and security domain. All.

Types of HIE. All.

Stakeholders primarily affected. Consumers, state agency, public health, providers.

HIE barriers addressed. All.

Stage of development. Implementation

Extent to which solution is in use. Public education efforts are underway. The Utah Department of Health maintains a public Web site geared to the consumer designed to inform consumers of their rights and ways in which their health information

can be used to improve consumer healthcare quality. In addition, many stakeholders have similar efforts underway. However, little emphasis is placed on the value or benefit to accessible personal health information.

Applicability of solution. Industry-wide.

Extent of barriers or opposition. Public education efforts are web-based and while it is estimated that a majority of the state of Utah has access, use and comprehension of web-based resources are not well documented.

Challenge - *Communicating with law enforcement the risks and realities of communicable disease encounters.*

Solution. Conduct joint training events for law enforcement and public health at annual conferences and seminars sponsored by local and state public health departments.

General Context. There is a need to enhance communication and education between law enforcement and public health regarding communicable disease transmission and associated risks for transporting infected persons.

Privacy and security domain. All.

Types of HIE. Public health.

Stakeholders primarily affected. Consumers, state agency, public health, law enforcement.

HIE barriers addressed. Cross-agency sharing, cultural.

Stage of development. Planning.

Extent to which solution is in use. Although many first responders receive training regarding the risk of working with

infected persons and need to take general precautionary measures, training is an ongoing process. Officer cadets receive instruction as part of the certification however, refresher courses are necessary to keep frontline responders well-informed of the true risks and recommended precautions to keep themselves and others safe.

Applicability of solution. Cross-agency training.

Extent of barriers or opposition. Coordination, identification of joint training priorities, on-going communication.

LEGISLATIVE

Challenge - *Regulatory requirements that distinguish certain classes of personal health information as more “sensitive” requiring different security measures thus creating barriers to exchange.*

Solution. All health information should be treated with the same standard for privacy and security when used and/or disclosed for the purpose of providing treatment and obtaining payment for such treatment.

General Context. There is concern that certain types of information such as that related to sexually transmitted diseases, mental health treatment, genetic testing results and substance abuse treatment have a risk for misuse that could cause significant harm to the patient. However, such misuse is most likely to occur when the information is used and/or disclosed for purposes other than treatment. There is a significant benefit to patients when all relevant health information, regardless of type, is made easily available for treatment purposes. Ensuring the adoption of industry-wide standards for health information exchange that maintain privacy and security can mitigate the risk of harm. Laws can exist to provide protections for sensitive personal health information, without placing restrictions on the

use of information for legitimate treatment purposes. See Mental Health Professional Practice Act (UC 58-60-114) and Genetic Testing Privacy Act (UC 26-45).

Privacy and security domain. All.

Types of HIE. All.

Stakeholders primarily affected. All.

HIE barriers addressed. All.

Stage of development. Federal initiative - stage unknown.

Extent to which solution is in use. N/A.

Applicability of solution. Simplification of regulatory requirements for exchanging health information.

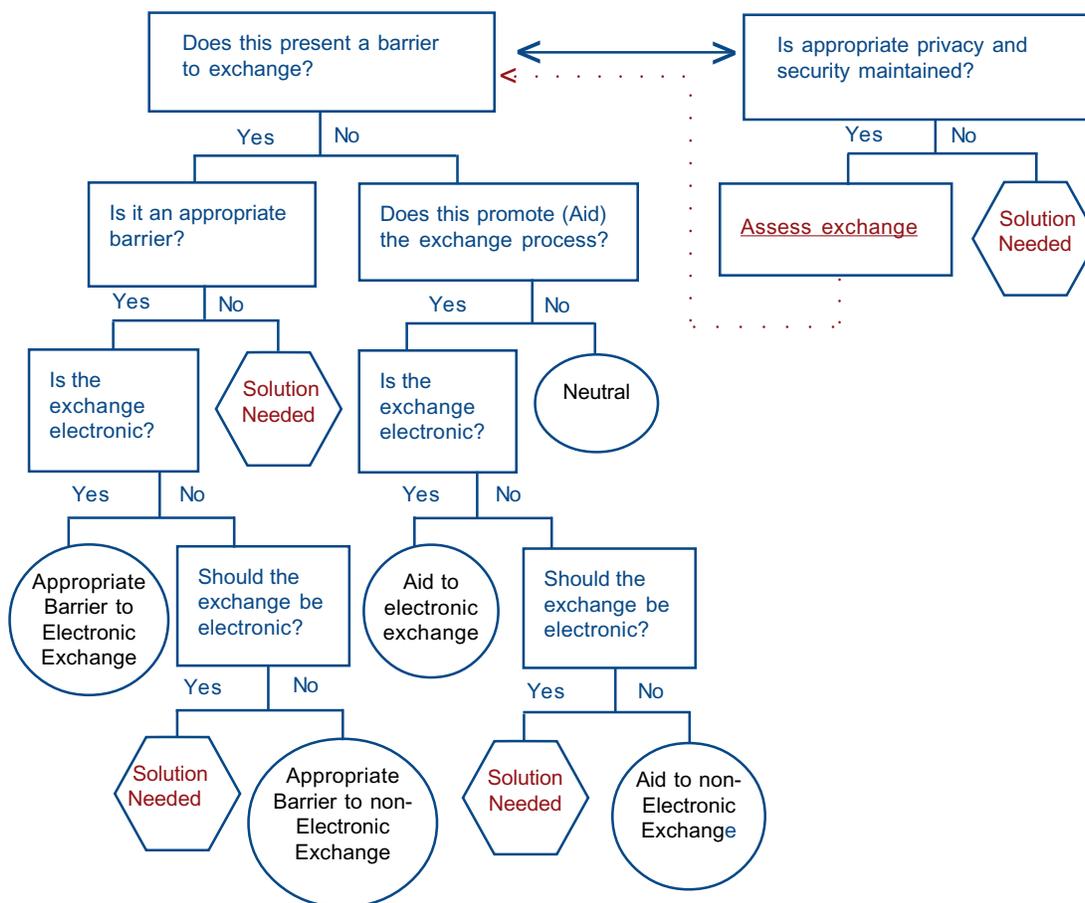
Extent of barriers or opposition. The primary barrier is 42 CFR Part 2 which governs substance abuse treatment records and restricts the use of these records for treatment purposes.

ATTACHMENT

A. Identification and Selection - Decision Tree

Purpose: Identify and evaluate solutions that:

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



- Barrier: Identified obstacles to the exchange of health information.
- Appropriate Barrier: Obstacles to the exchange of health information that are appropriate and maintain security and privacy.
- Aid: A business practices that promote the exchange of health information and maintains appropriate security and privacy.
- Neutral: Business practice has no impact on the exchange of health information.

REFERENCES

¹ Samore, M.H., Bateman, K., Alder, S. C., Hannah, E., Donnelly, S., Stoddard, G. J., Haddadin, B., Rubin, M. A., Williamson, J., Stults, B., Rupper, R. and Stevenson, K. (September 2005). Clinical Decision Support & Appropriateness of Antimicrobial Prescribing: A Randomized Trial in Utah and Idaho JAMA. 294: 2305-2314.

² NEDSS and NEDSS PAMS Business Discovery Statement Version 1.2 – 021202. (March 2002). Centers for Disease Control. Obtained 12/7/2006 from http://www.cdc.gov/nedss/BaseSystem/NEDSSBusinessDiscoveryStatement1_2.pdf.

³ Prehospital OnLine Active Reporting Information System Overview. Utah Department of Health. (August 2006). Obtained 12/7/2006 from <http://health.utah.gov/ems/data/polaris/overview.html>.

⁴ Nangle, B. & Talboys, S. (September 2002). Identifying Sharable Data in the Utah Department of Health. Obtained 12/12/2006 from <http://charm.health.utah.gov/publications.html>.
