



Interoperable Solutions for Health Information Exchange in Utah: A Final Report.

March 2007

Utah's Network for
Public Health Electronic Information-
Privacy and Security Project

Submitted by:

Lois Haggard, PhD, Project Director
Utah Department of Health
PO Box 14201
Salt Lake City, UT 84111

Submitted to:

Cynthia Irvin, PhD, State Liaison
Privacy and Security Solutions for
Interoperable Health Exchange
Research Triangle Institute
PO Box 12194
3040 Cornwallis Rd
Research Triangle Park, NC

Contract No. 290-05-0015

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

Executive Summary	1
1.0. Purpose and Scope	3
1.1. Purpose of Report	3
1.2. Background	3
1.3. Utah Health Information Technology	3
1.4. Report Limitations	6
2.0. Assessment of Variation	7
2.1. Methodology	7
2.2. Summary of Relevant Findings	7
2.3. Scenarios	8
2.3.1. Treatment	8
2.3.2. Payment	14
2.3.3. Regional Health Information Network (RHIO)	15
2.3.4. Research	15
2.3.5. Law Enforcement	17
2.3.6. Prescription Drug Use/Benefit	18
2.3.7. Healthcare Operations/Marketing	20
2.3.8. Bioterrorism	21
2.3.9. Employee Health	23
2.3.10. Public Health	24
2.3.11. State Government Oversight	26
2.4. Summary of Critical Observations	27
3.0. Solutions	28
3.1. Summary of Assessment of Variation	29
3.2. Effective Practices	30
3.3. Variation Not Addressed by Solutions Work Group	31
4.0. Analysis of Solutions	31
5.0. State Solutions	32
5.1. Solutions Work Group	32
5.2. Identifying Solutions	32
5.3. Inappropriate Scenarios or Exchanges	34
5.4. Vetting, Evaluating and Prioritizing Solutions	35
5.5. Organizing and Presenting Solutions	35
5.6. Determination of Feasibility	39
6.0. Analysis of Proposed Solutions	41
6.1. Solutions to Variations in Business Practices and Policies	41
Technological	41
Administrative	48
Legislative	49
Educational	50
6.2. State Privacy and Security Laws/Regulations	51
6.3. Contradictory Federal and State Laws/Regulations	51
6.4. Interstate e-Health Information Exchange	51
7.0 National Level Recommendations	51
Appendices	
A. RTI Standard Scenarios	53
B. Participating Stakeholders	61
C. Business Practice Data	64
D. Work Group Members	94
E. Business Practice Data Map by Scenario	98
F. Solution Work Group Decision Tree	117
G. Legal Reference Guide	119
References	133

Executive Summary

Beginning in July of 2006, the Utah Network for Electronic Public Health Information, Privacy and Security (UNIFY-PS) Project began collecting data from Utah's healthcare community regarding health information exchange business practices, policies, and state laws. This report is the third in a series that documents the efforts of the project workgroups to identify constraints on appropriate exchanges of health information, privacy and or security risks, and solutions that balance privacy and security and facilitate appropriate exchanges of health information while ensuring patient rights.

Utah's healthcare industry is in transition from a paper to an electronic environment and requires policies supportive of a phased migration. The findings refine and expand on the two previous interim reports; Assessment of Variations and Interim Solutions offered by the Variations Workgroup (VWG) and Solutions Workgroup (SWG). As such, the report consists of six major sections:

- Background and Purpose
- Assessment of Variation
- Summary of Key Findings from Assessment of Variations
- Review of State Solution Identification and Selection Process
- Analysis of State Proposed Solutions
- National-Level Recommendations

The data for this report was collected from a volunteer nonrandom sample of Utah healthcare stakeholders that were determined to have knowledge or engage in business practices relevant to each scenario. Care was taken to include diverse representatives from (urban and rural areas, differing size, profit/nonprofit, inde-

pendent) Utah to provide a comprehensive report of interoperability privacy and security.

The VWG met to determine which of the 154 business practices collected served as a barrier, without judgment, to HIE within the state. From these meetings three key findings emerged:

1. Health care providers obtained patient authorization to disclose health information for all situations except emergency situations.
2. Variations existed regarding the methods used to transmit protected health information with facsimile transmission being the most common. Variation further existed with regards to beliefs and understanding of transmission security.
3. Rules and statutes varied with regards to protected health information (PHI) and, as a result, entities implemented business practices according to a variety of legislative guidelines. Those guidelines primarily included either HIPAA or CFR 42 Part 2.

The Legal Work Group determined that a few business practices were driven by state statute. Utah Privacy or Tort Law was cited more often as a constraint in that organizational practices were defensive measures put in place to protect against tort litigation.

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 requires developing infrastructure capacity to support interoperability. Utah's history of public/private partnership demonstrates a commitment to open market solutions. While the proposed solutions represent only one network, a stra-

tegic planning effort must include all players in the healthcare industry as well as vendors and other entities that bring vital resources to the table. An open dialogue is needed to gain common understanding if we are to succeed in communicating with other agencies and organizations while maintaining privacy and security.

The solutions presented in this document are intended to preserve essential privacy and security protections, establishing a foundation for consumer trust with a patient's bill of rights and moving forward electronic connectivity to permit appropriate exchange of health information.

1.0 PURPOSE and SCOPE

1.1 Purpose of Report

Different patient care needs and interpretations of Health Insurance Portability and Accountability Act (HIPAA) have spawned variations in business practices and policies across healthcare organizations that sometimes work to inhibit exchange of clinical information. The purpose of this report is to document organizational business policies, practices, and state laws that may constrain the private and secure electronic exchange of health information and discuss proposed strategies and to facilitate appropriate health information exchange between healthcare industry stakeholders.

1.2 Background

In September 2005, the Agency for Healthcare Research and Quality (AHRQ) awarded an 18-month, \$11.5 million contract to Research Triangle Institute (RTI), International in a national effort to address privacy and security policy questions regarding Health Information Exchange (HIE) ¹. The Privacy and Security Contract term was then extended to 19 months, and the funding increased to \$17.23 million. This award is driven by national efforts to achieve medical interoperability as well as explore the possibility of a National Health Information Network (NHIN). To coincide with the exploration of these technological advances, President Bush released a 2004 directive for interoperable electronic health records by 2014 and subsequently created the Office of the National Coordinator for Health Information Technology (ONC) ². Under the contract, RTI, along with the National Governors Association (NGA) Center for Best Practices, implemented its Health Information Security and Privacy Collaboration (HISPC), under which it subcontracted with 33 States and Puerto Rico to assist them with doing the following:

- Identify variations in organization-

level business privacy and security policies and practices that affect electronic clinical HIE;

- For those practices that States considered desirable, documenting and incorporating them into proposed solutions;
- For those with a negative impact, identify the source(s) of the policy or practice and propose alternatives;
- Preserve privacy and security protections as much as possible in a manner consistent with interoperable electronic HIE;
- Incorporate State and community interests, and promote stakeholder identification of practical solutions and implementation strategies through an open and transparent consensus-building process; and
- Leave behind in States and communities a knowledge base about privacy and security issues in electronic HIE that endures to inform future HIE activities.

Throughout the summer and fall of 2006, the Utah Privacy and Security Project, Utah Network for Electronic Public Health Information Privacy and Security (UNIFY-PS), under the direction of the Utah Digital Health Services Commission (UDHSC) ³, engaged stakeholders from healthcare, law enforcement, public health, consumer and other realms in a discussion to examine privacy and security issues related to HIE.

1.3 Utah Health Information Technology

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 e-Health⁴, 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. The Utah Department of Health's Executive Director, Dr. David Sundwall, has praised the technological advances in health information interoperability⁵ and has been appointed to serve on the newly created, and NGA-

sponsored, "State Alliance for e-Health."⁶

UNIFY, a Utah Department of Health (UDOH) Center for Health Data project funded by the Robert Wood Johnson Foundation, is developing a plan for new systems in the areas of making perinatal electronic medical records (EMR's) interoperable with the Utah Birth Certificate, the exchange of standard immunization records between the Utah State Immunization Information Systems (USIIS) and clinical EMR's, and disease surveillance using electronic laboratory results data. The technology for these avenues of interoperability was established by the partnering of the University of Utah, Intermountain Health Care (IHC), and the University of Pittsburgh following a demonstrated need for syndromic surveillance during the 2002 Winter Olympics in Salt Lake City.

In 2004, UDOH was awarded a multi-year multimillion dollar contract from AHRQ to partner with the Utah Health Information Network (UHIN) and demonstrate a business case for clinical exchange in Utah. This funding is enabling UHIN to leverage its systems for the exchange of claims data to support the transmission of clinical, rather than administrative, data. Pilot projects are currently underway for the exchange of discharge summaries between hospitals and physicians, patient history and physical exams between physicians and hospitals, laboratory results between labs and physicians, and medication histories among health plans, physicians, pharmacies and hospitals.

Similarly, in 2006, the University of Utah established the Center for Excellence in Public Health Informatics as supported by a three-year Center for Disease Control (CDC) grant submitted jointly by researchers at the University of Utah Department of Biomedical Informatics, IHC, and UDOH staff. Collaborative projects funded through the center include real-time clinical electronic notifiable disease reporting, research on the prevention of deaths and adverse events due to non-illicit drug use, and improved linkage of patient immunization records in the statewide immunization registry.

The primary partner of the Utah Department of Health in this Privacy and Security initiative, HealthInsight, entered into a three-year contract with the Centers for Medicare & Medicaid Services (CMS) in mid-2005 to help physicians assess the benefits and overcome barriers to adopting and using Electronic Health Records (EHRs) and other health information technology. As part of the Doctors Office Quality Information Technology (DOQ-IT) project, HealthInsight is working with physicians to understand the potential of health information technology such as e-prescribing, electronic management of lab results, electronic medical image storage and transmission, and deployment of full electronic health records for improving care in ambulatory settings where most patient care is provided. HealthInsight will encourage adoption of HIT by helping physicians in Utah and Nevada learn about the clinical advantages of using EHRs for managing and improving care.

Other active Health Information Technology (HIT) efforts of the Utah Department of Health include the Utah Patient Safety Program, re-engineering of the Medicaid Management Information System, Immunization Registration, and the Children's Health Advanced Records Management (CHARM), child health information integration program. In addition, the Utah Bureau of Epidemiology currently collaborates with UHIN to expand the Remote Outbreak Detection System (RODS), which was implemented during the 2002 Salt Lake City Winter Olympics to conduct syndromic surveillance in Utah emergency rooms and pharmacies.

Utah has a long history as a center for the development and use of information technology to support health care delivery. *3M Health Information Systems* was established in Salt Lake City in 1983 and today is a world leader in medical records coding and computerized patient records. Utah's largest private health system is Intermountain Healthcare, a pioneer in the use of computerized patient records in hospitals and the electronic medical record (EMR) in clinical practice. Intermountain

Healthcare has ranked as one of the nation's 100 Most Wired health systems for five consecutive years, by American Hospital Association's *Hospitals & Health Networks* magazine. Utah has also been a leader in biomedical informatics research, since the founding of the Department of Medical Informatics in 1972 at the University of Utah.

Utah also has a somewhat unique twelve-year history of our health care stakeholder community coming together through UHIN to agree on standards for the exchange of electronic health care information. Prior to the nationwide adoption of the HIPAA electronic data interchange standards, insurers, hospitals, physicians, state government and other stakeholders came together and, in a process that took several years, developed a consensus on standards for the exchange of the administrative data necessary to process electronic claims. The group of trading partners opted to stay within the American National Standards Institute (ANSI) X12 framework and, as a result, influenced the national standards that were ultimately adopted under HIPAA. The trading partners eventually became the nonprofit UHIN Board of Directors, which is now comprised of representatives of 17 insurers, provider organizations and other interested parties, including state government. In 2004 the UHIN Board approved the formation of a number of new technical and governance committees to develop models for the exchange of clinical information. As a result, scores of individuals representing their organizations are currently engaged actively in developing a new community consensus on the foundations for a system of clinical exchanges.

A measure of the maturity of HIT initiatives in Utah is that the state's focus is now arguably on sustainability. UHIN has endured as a community resource for the exchange of administrative data in no small measure because of its self-sustaining business model. Trading partners pay either membership or transaction fees to participate in the

network of exchanges. Over time, the increased efficiencies of electronic commerce have resulted in savings to participants, as well as reductions in the transaction fees necessary to sustain the network. There is a consensus in the stakeholder community that clinical exchanges must be similarly self-sustaining through contributions of those engaged in the exchange of clinical health information. A primary focus of stakeholder workgroups is always developing the business case, along with the technical model, for new applications of health information technology. A second indicator of the maturity of the community's approach to HIT is the acceptance of the importance of standards as the basis for the exchange of electronic health information. Currently, 34 community-based health care data standards have been issued in regulations by the Utah Insurance Department, which is required by state law to adopt standards for health care claims and related issues. Each of these has been developed through a voluntary deliberative process that is sponsored by the UHIN Board, but is open to anyone who wishes to participate. Again, Utah standards are all developed within the framework of national standards to avoid creating an idiosyncratic regional market. The Utah healthcare stakeholder community has been actively engaged for over a decade in sorting through issues associated with HIT. It is a community accustomed to reliance on openly developed standards as the basis for health information exchange, leaving private technology vendors the task of aligning health care applications with the standards. Despite this level of HIT sophistication in the Utah stakeholder community, the rate of adoption of EMR in Utah has been very similar to the United States as a whole. Obviously, there continue to be barriers to the use of current HIT in clinical healthcare; no doubt the same barriers, including privacy and security-related barriers, that health care providers experience elsewhere. So, it is important that the Utah stakeholder community engages in this dialogue over the privacy and security infrastructure that is necessary to facilitate progress in the widespread adoption of EMR and other health information technology.

Patients in rural areas of the state also 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 departments⁵. 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 the EMR. 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 over prescribe 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 an email.

As Utah moves e-Health forward, it becomes critical to define with whom, and under what conditions, HIE interoperability is achieved.

1.4 Report Limitations

Serving as an impediment to the data collection process was the perception, on the part of the researchers involved, that a vested stakeholder interests in HIE ultimately may have resulted in a precautionary approach to defining business practices as barrier, neutral, and aid, as well as providing solutions and suggesting implementation. It was determined by the researchers that the outcome of this project could possibly be viewed as an infringement on livelihood or a critique of business model.

Furthermore, it was noted that several of the scenarios were not applicable to the exchange of electronic PHI as it occurs in the state of Utah and that during the combined Work Group process additional barriers were identified and information collected. For example, scenarios six and 18 were not seen as applicable, a payer would not request access to medical charts (see scenario five - payment), and disagreement was noted between emergency room physicians for handling requests for patient information (see scenario one - patient care A).

To further limit the research findings, the VWG asked stakeholders to consider electronic exchange in what is primarily a paper-based environment. As it stands, HIE on an electronic basis is mostly done by providers and payers utilizing UHIN to exchange administrative data in the processing of claims. Little, if any, clinical data is exchanged electronically in the state of Utah.

2.0 ASSESSMENT OF VARIATION

Phase one of this project assessed the degree to which variation existed among stakeholder business practices regarding the exchange of health information. To accomplish this, the 18 standardized scenarios were delivered to 77 stakeholders (See Appendix B) and from this 142 business practices were derived (N = 142; see appendix C). These business practices were further divided into three categories: Neutral (n = 42), Aid (n = 56), or Barrier (n = 44).

2.1 Methodology

Sponsored by HealthInsight⁸, Utah, and chaired by John Nelson, MD⁷, the Variation Work Group (See Appendix D) conducted a broad canvas of Utah's healthcare community and identified current privacy and security business practices and policies regarding exchange of personal health information. Members of this group, along with additional healthcare community stakeholders, identified variations in business practices and policies that presented barriers to electronic exchange of protected health information (PHI).

The ad-hoc VWG began to recruit stakeholders based on guidance outlined in the original proposal by RTI International and the NGA. Release of the 18 scenarios indicated that additional stakeholders were needed to collect all pertinent business practice data. The ad-hoc VWG then recruited additional stakeholders to match the stakeholder requirement of each scenario. This allowed for more accurate portrayal of business practice. Multiple methods to collect business practices from across the state were used with efforts being made to create a representative sample of the state (e.g., rural vs. urban, large vs. small). Over 100 stakeholders were contacted by telephone, with 77 participating in the collection of business practices. Efforts were made to ensure respondent

confidentiality and anonymity, although the intimate nature of the state often revealed stakeholder identity to varying work group members. Following telephone contact, participating stakeholders received an email survey. The survey contained detailed instructions, the applicable scenario, and specific questions tailored to the stakeholders' setting. The questions were designed to investigate, in depth, the stakeholders' business practice. Email also provided an opportunity for individual stakeholders to attach applicable policies with their response. In many cases, the variation group members and project team conducted a follow-up phone interview or continued with email correspondence to clarify or confirm the business practice(s) in question. In other instances, the project team visited stakeholders and conducted face-to-face semi-structured interviews.

2.2 Summary of Relevant Findings

- Information use and disclosure for treatment, payment, and healthcare operations was understood and, while allowable under HIPAA without authorization, most providers still requested patient authorization as part of the disclosure process.
- Information transmission or exchange security protocols were in place, but varied by provider and stakeholder entity. There was a general acceptance of mail, but fax was the overriding practice. Some larger entities had the capability of automated encryption for email transmittal yet not everyone had a means of secure email capability or trusted email transmission of PHI.
- Differential application of 42 CFR Part 2 consent requirements and HIPAA provisions for use and disclosure was difficult to untangle. When did 42 CFR Part 2 apply and under what conditions?

In a treatment setting most healthcare professionals understood the HIPAA treatment,

payment, and healthcare operations provision that provided for disclosure without patient authorization. Yet even given that allowance, in a non-emergency situation, providers or facilities more often than not requested that patient authorization be obtained as part of the disclosure process. The explanations for why this occurred included a requirement by the holder of the record, a defensive or protective measure against malpractice or privacy lawsuits, or a good consumer-conscious practice.

Transmission and exchange of information typically occurred by whatever means was most expedient given the situation. Healthcare providers across the state had a general familiarity with exchange partners' methods of communication and adapted to what was necessary to continue the treatment of the patient. In Utah, facsimile transmission was the most commonly used mode of transmission. In most long-term care facilities surveyed it was noted as being the only means for exchange. Many hospitals, on the other hand, had more sophisticated systems with automatic encryption when the string "PHI" was detected in the subject line of an email.

2.3. Scenarios

Business practice data was collected from 77 Utah stakeholders (e.g., hospitals, physicians, pharmacies, laboratories, payers, law enforcement, EMS, state agencies, public health and consumers) using 18 standardized scenarios. The scenarios detail a mix of health care information exchange situations including:

- patient care (one through four);
- payment (five);
- regional health information exchange-RHIO (six);
- research data use (seven);
- access by law enforcement (eight);
- pharmacy benefits (nine and ten);
- healthcare operations and marketing (11 and 12);
- bioterrorism (13);
- employee health information (14);
- public health (15, 16, and 17); and
- health oversight (18).

While all 18 scenarios were not applicable to the state of Utah, responses were modified or elaborated on if a similar or slight variation of the scenario would be more likely to take place. Any deviation from the original scenario was noted.

2.3.1. Treatment

[Scenario 1 Patient Care A](#)

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89-year old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. There are questions concerning her possible impairment due to medications. Her adult daughter informed the ER staff that her mother has recently undergone treatment at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines there is a need to obtain information about Patient X's prior diagnosis and treatment during the previous inpatient stay.

[Scenario 2 Patient Care B](#)

An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The two organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol relevant for medical diagnosis. The requested substance abuse information is being sent to the primary care provider. The primary care provider intends to refer the patient to a specialist and send all of his/her information including the substance abuse information received from the substance abuse treatment facility to the specialist.

[Scenario 3 Patient Care C](#)

5:30pm Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psych unit to the nursing home. The hospital and skilled nursing facility are separate entities and do not share electronic record systems. At the time of

the patient's transfer, the discharge summary and other pertinent records and forms were electronically transmitted to the skilled nursing home.

Upon entering the facility Dr. X seeks assistance in locating his patient, gaining entrance to the locked psych unit and accessing her electronic health record to review her discharge summary, I&O, MAR and progress notes. Dr. X was able to enter the unit by showing a picture identification badge, but was not able to access the EHR. As it is Dr. X's first visit, he has no login or password to use their system.

Dr. X completes his visit and prepares to complete his documentation for the nursing home. Unable to access the skilled nursing facility EHR, Dr. X dictates his initial assessment via telephone to his outsourced, offshore transcription service. The assessment is transcribed and posted to a secure web portal.

The next morning, from his home computer, Dr. X checks his email and receives notification that the assessment is available. Dr. X logs into his office web portal, reviews the assessment, and applies his electronic signature.

Later that day, Dr. X's Office Manager downloads this assessment from the web portal, saves the document in the patient's record in his office and forwards the now encrypted document to the long-term care facility via email.

The skilled nursing facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

[Scenario 4 Patient Care D](#)

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State

A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the BrCa gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

2.3.1.a. Stakeholders

Hospitals. The majority of stakeholders responding to treatment scenarios one through four were hospital affiliated respondents (n = 7) including a privacy and quality improvement officer, an emergency room physician at a tertiary hospital, as well as radiological staff, file clerks, and breast care coordinators at several tertiary hospitals. Hospital respondents were involved in answering scenarios one and four. The single hospital stakeholder for scenario three is the manager of the HIPAA privacy office for an integrated delivery system.

Community Clinics. While the center manager and director of a community clinic also responded to scenario four, the remainder of community clinics (n = 5) answered scenario two. The unique nature of Utah's healthcare system showed an overlap in community clinics and health centers that serve as homeless shelters and provide care for substance abuse and mental health patients. These respondents included the director of a private, nonprofit program and the executive director at a state-licensed substance abuse treatment center. Also included in community clinic and health center respondents were a physician and medical director whose clinic is part of an integrated delivery system, as well as an office manager at a residential eating disorder facility.

Public Health Facilities. The public health agency that responded to scenario two receives a combination of government, private foundation, and individual contributions. Respondents for the public health agency included its director and a practicing physician assistant.

Clinicians. The clinician represented the chairman of the department of psychiatry at a tertiary hospital who also maintains a private practice and serves as faculty at a medical and public health school that undertakes research.

Long-Term Care Facilities. Respondents to scenario three included the chief executive officer at a not-for-profit senior care facility and the financial service consultant for rehabilitation and extended nursing care facility.

2.3.1.b. Domains

Information Authorization and Access Controls. In treatment scenarios one through four, the privacy and security domain that listed the greatest number of business practices was in regards to information authorization and access controls (n = 15). It was found that, within this domain, variation exists with regards to the urgency of the scenario, the information being exchanged, and the individual identity of the stakeholders involved.

Access to PHI was granted with the least amount of difficulty to those working in an emergency medical environment. In those situations, security administration policies and procedures existed that would allow an individual to access electronic and paper PHI based upon their role and responsibility. As the level of care and priority of treatment became less critical, access and authorization became more guarded between entities called upon to share PHI, specifically in the instances regarding access to substance abuse information.

PHI containing a history of substance abuse was shared, following patient authorization, according to the specifics of 42 CFR Part 2, which details what information is to be exchanged, between what parties, and for what period of time. This “minimum information sent” was described by a physician’s assistant as having “little utility” and therefore was disregarded in favor of obtaining the patient’s history of substance abuse directly from the patient. This notion of “little utility” was again voiced by a general

care practitioner who indicated that a specialist would determine what information was needed and initiate the request for PHI with the substance abuse patient being physically in the specialist’s office. Just as HIPAA contains a “minimum necessary” disclosure mechanism and the Privacy Rule allows for communication on a “need-to-know” basis, 42 CFR Part 2 contains a consent-driven disclosure mechanism that requires the communication of information within the program (or to an entity with direct administrative control over the program) to be limited to those persons who have a need for the information in connection with their duties that arise out of the provision of diagnosis, treatment or referral for treatment of alcohol or drug abuse. (See 42 CFR § 2.12).

In a long-term care facility, access to electronic and paper PHI was dependent on the stakeholder involved. Physicians and other health care providers with required credentials would be granted temporary access to their patient records on a “need to know” basis. The majority of respondents to scenario three indicated access to protected health information was obtained electronically with a login and password. In a long-term care facility, access to electronic and paper PHI was dependent on the stakeholder involved. Physicians and other health care providers with required credentials would be granted temporary access to their patient records on a “need to know” basis. The majority of respondents to scenario three indicated access to protected health information was obtained electronically with a login and password. There was variation noted among long-term care facilities’ practices for granting physicians temporary access to their facility and records system but facilities have procedures in place should temporary access be necessary under such situations. The sharing of patient information differed from entity to entity with some requiring that a business associate agreement be in place and others indicating such agreements are not necessary between providers involved in the treatment of a patient. This was

specifically the case when the access of information was between the long-term care facility and physician when compared to an exchange between physicians. While a business agreement was identified as the correct practice when a physician served as a consultant to the long-term care facility, a business agreement was not required for a physician involved in the treatment of patients at the long-term care facility.

The long-term care facility could grant a health care provider access to patient records when appropriate via an electronic system at the discretion of the long-term care facility. Long-term care facilities operating electronic medical records required technical safeguards including unique user identification and procedures for accessing electronic PHI in an emergency. This were true even if access were temporary. (See 45 CFR § 164.514:(d)(2)(i); § 164.312).

Information Transmission Security or Exchange Protocols. Little variation in transmission and transmission security was evident among the major stakeholders in the health care community of Utah with the exception being security measures employed by substance abuse treatment facilities. Long-term care facilities predominantly used electronic fax as their method of choice for health information transmissions as do hospitals, physician offices, and other major stakeholders. Less utilized means of transmission included mail, courier, and patient pickup. The large hospitals and the integrated delivery systems stated having the ability to use encrypted email, but this method was not yet widely used and/or accepted. A stated reason for this was that many facilities have policies in place that prohibit email use for transmitting patient information.

The sensitivity of the information being transmitted notably influenced the security measures employed. Substance abuse providers noted that they would verify the entity requesting substance abuse PHI,

ask the receiver to stand by the fax machine, stamp the fax cover sheet with "re-disclosure prohibited," attach the full CFR 42 Part 2 re-disclosure prohibition with the fax, and require a follow-up fax acknowledging receipt. When disclosing PHI to an individual, one treatment facility reported they required a signed receipt that would be placed in the patient record. These more stringent measures stood in contrast to physicians who reported they regularly disclosed patient information over the phone once they were confident they were talking to an appropriate caregiver. How confidence was obtained was never fully verbalized, rather it was suggested that the conversations that took place would be those that would only occur between physicians. As such, physicians were able to forward patient information without patient authorization or consent (much to consumer surprise, who was under the impression that consent was required). What CFR 42 Part 2 does not entail is the transmission of PHI. Only HIPAA gives general guidelines that include: 1. Covered entities use appropriate administrative, technical, and physical safeguards to protect the privacy of PHI; and 2. Covered entities to have policies and procedures in place that are reasonable and appropriate to comply with the Security Rule. (See 45 CFR §164.530 (c)(1); § 164.306).

The electronic methods (CDs and the Internet) are used commonly with other radiology films (e.g., x-rays) in Utah, especially among large facilities. Mammography films were a unique case in Utah as the technology for digital mammograms has not been fully accepted and implemented. Until recently, most physicians did not feel comfortable with the resolution of electronic mammography films and while some facilities now have the capability to make CDs and use the Internet (by PACS, picture archiving and communication system) to transfer mammography films, they reported rarely utilizing these methods. It was found more common to transfer films by the patient or patient representative hand-carrying them or to send films by U.S. mail. At one mammography file room, the file clerk reported that they require a twenty-four hour notice on all film requests to allow for the processing of the patient film and record and that any individual attempting to obtain the film present

an approved form of identification.

User and Entity Authentication. Little variation was reported regarding the treatment scenarios when detailing business practices that would authenticate a person or entity seeking access to PHI. Hospitals, community clinics, and substance treatment facilities commonly accepted a fax request on letterhead as a form of authentication and often disclosed information over the phone as providers are usually familiar with one another and referral is common. In one hospital emergency room, a physician noted that when requests involved emergency situations, he asked for a national physician identification number. In addition, the emergency room physician stated use of the Internet to verify the requesting facility. This was determined to not be an extensive practice however as that majority of providers questioned stated that they accept requests for PHI as common occurrence. One substance abuse treatment facility reported using a signed receipt from the requester of all medical information at their facility, regardless of delivery method.

While Utah State Code does not require authentication, HIPAA specifies that covered entities receiving a request for patient medical records authenticate the identity of requester prior to sending medical information. HIPAA does not specify what steps are required to verify. If reasonable steps are taken, the disclosing covered entity is entitled to rely on the verification. See 45 CFR § 164.312 (d)(e); § 164.514(h)].

Administrative or Physical Security Safeguards. Administrative or physical security practices to secure patient health information varied widely given the entity and scenario. Training in data security was noted as a requirement for each staff member, including volunteers, at one responding hospital. Conversely, community clinic/public health agency employees and volunteers with direct access to patient charts/records reportedly were required to sign confidentiality agreements prior to access while long-term care facilities and most hospitals require a login and password for all staff with access granted on a “need to

know” basis. No one reported the use of sharable passwords.

The long-term care facility responding also stated that they could grant a health care provider access to patient records when appropriate. The decision to grant temporary access to the patient record via the electronic system was found to be at the discretion of the long-term care facility and any long-term care facilities operating electronic medical records required technical safeguards including unique user identification and procedures for accessing electronic PHI in an emergency. This was found to be true even if access were temporary.

Hospital safeguards were generally electronic in nature and included passwords and security access cards. Access to the facility and to patient records was linked to the identity of the individual staff member through electronic identification. Records systems in community clinics, public health agencies, and long-term care facilities tended to be paper-based and included locked and double locked doors. Substance abuse treatment facilities placed a higher degree of sensitivity on the substance abuse PHI by placing it behind double locked doors.

Information Use and Disclosure Policy. Utah business practices involving health care entities sharing clinical health information in a paper environment did not show variation across the treatment scenarios. Data gathered regarding information use and disclosure indicated that most covered entities preferred to get patient authorization to disclose patient health information with the exception of an emergency situation. Business practice data showed methods to account for disclosures including, but not limited to, signed receipts and requests that would be placed in the patients chart, information exchange logs, and verification of recipient.

State Law Restrictions. Particular to scenario four, Utah Code Ann. §78-25-26 stipulates who can be recognized as a personal representative to authorize access

to the medical records and information of a deceased relative. The release of the genetic information of a deceased patient is not accessible through the signed authorization of next of kin unless that person is the personal representative under Utah State Code. The release is allowable with the authorization of either a personal representative or the executor of the deceased's estate. There are no additional state law restrictions with regard to information types and classes by which electronic personal health information can be viewed and exchanged specific to the treatment scenarios.

2.3.1.c. Observations

Scenario One. When an emergency room physician is involved in an emergency situation and needs a patient's medical information, the physician reported efforts are made to access the patient's medical information without patient authorization. In emergency situations, hospitals reportedly disclosed information without authorization to a requesting covered entity once that entity was verified. This was not the case in the remaining three treatment scenarios. While physicians and hospitals noted authorization was not required, the overwhelming majority reported they would seek patient authorization prior to disclosure.

The release of patient information across state lines was not found to be a factor in the exchange of patient information. It is unclear what the requirements would be from neighboring states to disclose patient information. Hospitals responding within the state of Utah reported that in an emergency, the information request would be fulfilled following authentication of the requestor. If not an emergency situation the practice is to receive patient authorization to disclose.

Scenario Two. There were differences between providers' treatment of patient medical information when substance use was involved. There was variation reported in the treatment facilities', physicians', and integrated delivery systems'

understanding of 42 CFR Part 2, its relation to HIPAA, and the application of each. Treatment Facilities noted stringent precautionary measures to safeguard patient substance use information. While physicians commented on limited or restricted access to patient medical files, treatment facilities noted that patient files were kept in a locked cabinet behind a double locked door.

There was a general understanding of 42 CFR Part 2 by the treatment facilities responding to the scenario survey. However, the differences in the provisions under HIPAA and 42 CFR Part 2 were such that there is a lack of clarity around which regulation applies and under what conditions. The differences in language and drivers for each regulation added to the confusion and misapplication of the regulation.

Scenario Three. Long-term care facilities' had procedures in place to grant physicians temporary access to their facility and records system should temporary access be necessary. The policies and practices differed from entity to entity with some requiring that a business associate agreement be in place and others indicating such agreements are not necessary between providers involved in the treatment of a patient. Most information transmitted to and from long-term care facilities was done by fax.

Scenario Four. The majority of mammograms in the state were reportedly done on film; this was the case in both rural and urban facilities. One integrated delivery system used digital images for mammography and a second had plans to transfer to digital within the next two years. However, even at the integrated delivery system that used digital imagery, the images were printed in hard copy for the physicians as most institutions and physicians were not comfortable with digital film. Films were transmitted or exchanged by mail, courier, or to the patient with signed patient release. There was no stated policy or practice for exchanging information across state lines or when dealing with an HIV positive patient as precautionary measures would not differ given this condition. Requests from out of state facilities required an authorized release that is faxed or mailed. Utah Code 78-25-26

established regulations for release of medical information for a deceased relative.

2.3.2. Payment

Scenario 5 Payment

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the healthcare provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (e.g., emergency department records, clinic notes, etc.).

The health care provider has recently implemented an electronic health record (EHR) system. All patient information is now maintained in the EHR and is accessible to users who have been granted access through an approval process. Access to the EHR has been restricted to the healthcare provider's workforce members and medical staff members and their office staff.

X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

2.3.2.a. Stakeholders

Clinicians. A Health & Wellness Clinic responding as the clinician for scenario five specialized in the treatment of nerve, muscle and skeletal/spinal conditions. The clinic consisted of component parts (chiropractic care, therapeutic massage and acupuncture) to offer a complete alternative health care approach. The clinic served as a provider for most health insurance companies, as well as provided diagnosis and treatment of workers' compensation and auto injuries.

Payers. The three payers responding to scenario five were a regional healthcare IT specialist for a not-for-profit company that ranks as the largest health insurer in its geographical area, a privacy officer for the state retirement system, and a representative from state Medicaid. It was after the fact

that the SWG chair and director of Utah's Public Employees Health Plan determined that scenario five, as described, was not applicable. The reasons for this are described in 2.4.c. Critical Observations.

Consumer/Consumer Organizations. The consumer was a young mother who had changed jobs and had seen many different health insurance situations.

2.3.2.b. Domains

Information Authorization and Access Controls. Both payers and clinicians were in agreement on access to PHI in the payer setting. The main concept cited by both was that only the "minimum necessary" under HIPAA was given to the payer. How this happened varied based on the provider's technological capabilities. In the case of an EHR, special payment reports were created which gave the payer only the information it needed. In a paper-based records environment, the information was extracted from the paper chart by the provider and then sent to the payer. In like manner, the consumer who responded expressed concern that only the information that is needed should be shared.

Information Use and Disclosure. Variation was noted in Utah concerning need for consent to disclose information when dealing with payment issues. The providers generally obtained a consent or authorization for payment purposes. Payers reported that they had access to health information under HIPAA "treatment, payment and healthcare operations" and that consent was not needed. The payers reported the necessity to have agreements in place in order to work with providers. The consumer believed that an authorization is required for patient information to be disclosed.

2.3.2.c. Observations

Payers worked with the understanding that patient authorization is not needed for payment purposes. Payers also regularly engaged in agreements with health care providers to facilitate the payment process.

Health care providers showed variation in whether they obtained authorization from patients to allow access to patient information for payment purposes. Providers tended to err on the side of caution and more often obtained patient consent. As providers had different levels of EMR technology and comfort with this technology, the process by which payers accessed patient and billing information varied. Both payers and providers reported little variation in the description of what constitutes “minimum necessary” according to HIPAA.

It was further noted by the SWG chair and director of Utah’s Public Employees Health Program, that he knew of no instance whereby a payer would seek access electronically to a providers EHR database. This rendered scenario five obsolete by Utah standards.

2.3.3. RHIO

Scenario 6 RHIO

The RHIO in your region wants to access patient identifiable data from all participating organizations (and their patients) to monitor the incidence and management of diabetic patients. The RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients.

2.3.3.a. Stakeholders

Consumer/Consumer Organizations. The RHIO responding to scenario six was a nonprofit coalition of competing entities that provided secure, electronic information exchange connecting every payer and nearly every healthcare provider in the state of Utah. It operated as a “gateway” or “information highway” exchanging information between different entities. The RHIO did not view, store, edit, or evaluate the quality of data it received. Instead, the Utah RHIO functioned like a “post office” transferring information from the sender to the intended receiver.

2.3.3.b. Domains

The Utah RHIO operates in a very different paradigm than what is depicted in the scenario. No business practice data or domains are reported.

2.3.3.c. Observations

This RHIO scenario did not describe the services performed by the Utah RHIO. The Utah RHIO was a gateway or information highway where information was exchanged between different organizations. The Utah RHIO did not request or permanently store data. The Utah RHIO functioned instead like the post office in getting information routed from the sender to the intended receiver. The Utah RHIO did not perform quality measurements on its members’ data and has a standards committee that would charter a subcommittee to develop a community standardized message should members want to exchange/submit patient information from one organization to another.

2.3.4. Research

Scenario 7 Research Data Use

A research project on children younger than age 13 is being conducted in a double blind study for a new drug for ADD/ADHD. The research is being sponsored by a major drug manufacturer conducting a double blind study approved by the medical center’s IRB where the research investigators are located. The data being collected is all electronic and all responses from the subjects are completed electronically on the same centralized and shared data base file.

The principle investigator was asked by one of the investigators if they could use the raw data to extend the tracking of the patients over an additional six months and/or use the raw data collected for a white paper that is not part of the research protocols final document for his post doctoral fellow program.

2.3.4.a. Stakeholders

Clinician. Of the two research investigators responding to scenario seven, one was a licensed registered nurse designated

researcher-only with no obligation as faculty or affiliation with any company outside of the university. A medical and public health school that undertakes research employed this individual.

Physician Groups. The second researcher responding to scenario seven was a licensed pediatrician with a university-affiliated practice that also served as assistant professor of pediatrics. A medical and public health school that undertakes research employed this respondent as well.

Medical and Public Health Schools that undertake Research. Responding for the Institutional Review Board (IRB) was the Director of the IRB at a medical and public health school that undertakes research and served as the senior compliance consultant of an integrated delivery system. Both respondents had numerous years of experience serving on institutional review boards.

Consumer/Consumer Organizations. The health care consumer responding to scenario seven was the father of four children and spoke directly as if his 13 year-old child was involved in the study as presented by the scenario.

2.3.4.b. Domains

Information Use and Disclosure. All business practices in scenario seven were related to the privacy and security domain of information use and disclosure. The internal policies at the medical and public health school and at the integrated delivery system were both reported as established in accordance to 45 CFR HIPAA Privacy Rule.

The two researchers indicated that they (as principal investigator) would either pursue IRB approval for the extended use of data and a “white paper” or require the post-doc hoping to use the data to pursue IRB approval separately. One researcher specified that this IRB amendment would be required regardless of who owned the data the (i.e. the research school or the pharmaceutical company sponsoring the research study).

Variation was noted in the instance of seeking

parental approval for use of data beyond that originally included in the protocol approved by IRB. The chair of IRB at the medical and public health school that undertakes research indicated that a re-consent via a parental permission document and an updated assent for children aged seven to 17 would be required. The senior compliance consultant noted that the IRB would encourage the principal investigator to submit approval for a new project that was designated “data-only” and could thereby apply for a waiver of authorization as allowed for by the Privacy Rule. They also noted that this scenario would likely never gain approval by the IRB without the post-doctoral student initiating a new and revised IRB study document.

While the licensed nurse indicated that their business practice would coincide with the former practice of seeking a re-consent from the parent and re-assent from the minor, the pediatrician indicated that their first step would be to return to the original IRB document and determine if it stipulated the length of time for which data could be collected. They also indicated that they would check the original consent form to see if a clause was included that allowed for the use of secondary analysis to determine if it would be possible to check with IRB and ensure compliance rather than submit new paperwork.

2.3.4.c. Observations

With regards to the research data use provided in the scenario, the decision to resubmit to the institutional review board exhibited variation depending on responder. Even though it was implied that the drug company owned the data, the decision to resubmit was linked to authorship. If the principal investigator did not want to have ties to the secondary analysis he/she would request the post-doc to independently submit to IRB. Variation was also noted in the requirement of a parental re-consent and study subjects re-assent for the use of data beyond that originally included in the protocol approved by IRB. One researcher indicated that approval was

required while a second indicated that they would first search for prior authorization. More variation was demonstrated by the IRB suggestion that the project be submitted data-only and thereby negating the need for a re-consent and re-assent.

2.3.5. Law Enforcement

[Scenario 8 Access by Law Enforcement Scenario](#)

An injured nineteen (19) year old college student is brought to the ER following an automobile accident. It is standard to run blood alcohol and drug screens. The police officer investigating the accident arrives in the ER claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood alcohol test results and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff.

The patient is covered under their parent's health and auto insurance policy.

2.3.5.a. Stakeholders

Hospitals. Representing the hospital stakeholder for scenario eight was an emergency room physician at a tertiary hospital and the privacy officer of a medical center. The emergency room physician responding to scenarios one and eight served as a member of the VWG and SWG and as such responded to the scenarios, not in advance, but while discussing barriers and variations to business practices identified by the privacy officer and law enforcement personnel. The emergency room physician had been given the scenarios prior to the variations work group meetings however.

Law Enforcement. One individual representing the law enforcement stakeholder group was a detective that, similar to the emergency room physician, served on the VWG and SWG. In this

capacity, both detective and physician were able to identify further variation and barriers to business practices identified in scenarios one, eight, and 13. Another respondent to scenario eight was Chief of Police for a town with a population of less than 15,000.

Consumer/Consumer Organizations. The consumers for scenario eight were represented by a local undergraduate student and his family and, while consisting of opinion, allowed for moments of hilarity while demonstrating that an abundance of television was being viewed in the household.

2.3.5.b. Domains

Information Use and Disclosure. Most of the business practices in scenario eight focused on disclosing patient health information. A clear chasm existed between law enforcement and the medical community that prohibited the exchange of information. Law enforcement reported that they have officers collect as much information as possible prior to transporting an individual to a hospital. This was seen as a necessary operating procedure because once the individual entered a medical facility the difficulties law enforcement experienced in gathering information increased significantly. In addition, from a law enforcement perspective, most physicians were reluctant to talk because they didn't want to be involved in any legal proceedings.

Most physicians reported they could not disclose patient information without legal documentation to do so or without the patient's authorization.

2.3.5.c. Observations

Scenario eight highlighted the chasm that existed between law enforcement and hospital personnel with regards to communication. Hospital physicians were identified by law enforcement as not willing to disclose information without subpoena. This was believed to stem from a desire to avoid legal entanglements. Similarly, hospital physicians were very careful not to disclose information to parents and instead opted to let the patient inform parents of their medical information and/or consumption of alcohol. We found no

agreement between law enforcement and hospitals regarding who draws for blood alcohol levels or the subsequent measure thereof. The units of measure for a blood draw in a hospital were different from those of a paramedic, which adds another layer of complexity. Most law enforcement agencies would maintain business agreements with paramedics to perform blood alcohol draws at the scene of an accident and law enforcement was adamant that officers gather as much information as possible before the patient arrived at the hospital. The reason for this was identified as being a result of little, if any, information being gathered after the patient entered the hospital without initiating legal paperwork.

2.3.6 Prescription Drug Use/Benefit

[Scenario 9 Pharmacy Benefit Scenario A](#)

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy for a hospital which is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's Outpatient Clinic.

[Scenario 10 Pharmacy Benefit Scenario B](#)

A Pharmacy Benefit Manager 1 (PBM1) has an agreement with Company A to review the companies' employees' prescription drug use and the associated costs of the drugs prescribed. The objective would be to see if the PBM1 could save the company money on their prescription drug benefit. Company A is self-insured and as part of their current benefits package, they have the prescription drug claims submitted through their current PBM (PBM2). PBM1 has requested that Company A send their electronic claims to them to complete the review.

2.3.6.a. Stakeholders

Pharmacies. Pharmacy stakeholders were recruited with the aid of the director of the state pharmacy association, who identified a broad sampling of pharmacists. Three pharmacists responded – one from a managed care environment, one from an urban independent, and one from an urban grocery store chain. A rural pharmacist declined to participate, as he did not feel qualified. In addition to the pharmacy association contacts, an atypical pharmacist was also recruited. This pharmacist provides chemo, intravenous, in home and outpatient pharmacy services.

Community Clinics and Health Centers. An advanced practice registered nurse (APRN) with a licensed mental health clinic responded as a community clinic stakeholder for scenario nine. The responding practitioner owns the practice.

Consumer/Consumer Organizations. Three consumers participated in the pharmacy scenarios. They included an agent/broker for several self-insured employers, an employee of Workman's Compensation Fund of Utah and a physical therapist that specializes in elderly home care.

2.3.6.b. Domains

Administrative or Physical Security Safeguards. The use of administrative or physical security safeguards in scenario ten is exemplified by the initiation of a business associate agreement "outlining appropriate administrative and physical security practices" by the consumer organization to provide the pharmacy with information. Similarly, the pharmacy demonstrated the use of administrative or physical security safeguards by having "established business practices to reasonably ensure physical security," in this case, by only using data that has been de-identified.

Physician, pharmacy, and PBM use or disclosed protected health information for their own treatment, payment, or health

care operations (“TPO”), because all are presumably covered entities under HIPAA. [See 45 CFR § 164.506(c)(1)] In scenario 9, the physician, pharmacy, and PBM may each be viewed as a covered entity under HIPAA because each is a health care provider. [See 45 CFR § 160.103 (Covered entity)] The term “health care provider,” in turn, includes any person who provides health care or medical or health services in the normal course of business. [See 45 CFR § 160.103 (Health care provider)] Thus, as health care providers under HIPAA, physician, PBM, and pharmacy can freely interact with patient for “treatment, payment and healthcare operations” purposes, including obtaining additional information from a patient, or giving additional information to a patient. In addition, as healthcare providers, PBM, pharmacy, and physician can disclose patient information to each other and to other healthcare providers for treatment purposes. [See 45 CFR § 164.506(c)(2)] Thus, PBM, pharmacy, and physician can each talk to patient and to each other regarding filling the Geodon prescription without the need to obtain a patient authorization.

The PBM1 in scenario 10 is not providing a treatment purpose, but is carrying out a health care operations purpose for Company A. [See 45 CFR § 164.501 (Health care operations)] Company A is not permitted to disclose information to PBM1 for a health care operations purpose because PBM1 is either not a covered entity under HIPAA and/or because PBM1 does not have an independent relationship with the patient. [See 45 CFR § 164.506(c)(4)]

Given the circumstances illustrated in scenario 10, Company A needs either an authorization from the patients or needs to enter in a business associate agreement with PBM1 if patient identifying information is to be used. [See 45 CFR § 164.502(a)] The requirements of the business associate agreement are set forth in 45 CFR § 164.504(e)(2); the business associate agreement would typically be worded to permit PBM1 to

have access to relevant patient information only for the purposes of carrying out the specific assignment given by Company A. The minimum necessary rule would require that only de-identified/aggregated information be provided if that is sufficient to carry out PBM1’s assignment. [See 45 CFR § 164.514(d)]

If only de-identified information is provided, HIPAA would not require a business associate agreement. Additional contracts may be entered into between the parties (for example, the services agreement describing the services to be provided by PBM1 and the payment by Company A; or a nondisclosure agreement). These additional contracts are not required by HIPAA.

2.3.6.c. Observations

In scenario nine, variation was noted with regards to who contacts the patient to inform that the original prescription authorized is not on the formulary. In some cases the mail order pharmacy would contact the patient and in other cases it was the physician. Variation was also reported in the options offered to the patient given this situation (e.g., pay out of pocket for original medication or choose an alternate medication). Consistency was noted with regards to the agreement that a pharmacy would receive the “minimum necessary” information to fill their orders.

Variation existed in scenario ten with regards to whether a business associate agreement was required to share information between parties. The company seeking a cost comparison reported they would require a business associate agreement regardless of whether the data were de-identified. The pharmacy benefits manager did not feel an agreement was necessary if the data were de-identified.

HIPAA does not have special rules if the provider is in a different state than a PBM. Treatment, payment, and health care operations are not limited by state boundaries and the minimum necessary rule applies regardless of where the provider and PBM are located. State law or different state customs may impact the interaction between a provider and PBMs in different states. Insurance

companies and other payers may contractually impose pre-authorization, eligibility, or verification requirements on patients or PBMs. Patients may have different preferences about whether they like to present with the written prescription or have the physician's office submit it directly to the pharmacy.

2.3.7. Healthcare Operations/Marketing [Scenario 11 Healthcare Operations and Marketing A](#)

ABC Health Care is an integrated health delivery system comprised of ten critical access hospitals and one large tertiary hospital, DEF Medical Center, which has served as the system's primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports containing patient identifiable data to the system six-sigma team to analyze patient encounters and trends for the following rehab diagnoses/ procedures:

- Cerebrovascular Accident (CVA)
- Hip Fracture
- Total Joint Replacement

Additionally, ABC Health Care is requesting that this same information, along with individual patient demographic information, be provided to the system Marketing Department. The Marketing Department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

[Scenario 12 Healthcare Operations and Marketing B](#)

ABC hospital has approximately 3,600 births/year. The hospital Marketing Department is requesting identifiable data on all deliveries

including mother's demographic information and birth outcome (to ensure that contact is made only with those deliveries resulting in health live births).

The Marketing Department has explained that they will use the PHI for the following purposes:

- To provide information on the hospital's new pediatric wing/ services.
- To solicit registration for the hospital's parenting classes.
- To request donations for construction of the proposed neonatal intensive care unit
- They will sell the data to a local diaper company to use in marketing diaper services directly to parents.

2.3.7.a. Stakeholders

Hospitals. Answering as a hospital stakeholder for scenario eleven was the newly hired Director of Public Relations/ Marketing for the Orthopedic branch of an integrated delivery system, professor and Chair of the Orthopedic branch just mentioned, a privacy officer at an integrated delivery system, and two Directors of Nursing at separate medical centers. Representing the hospital stakeholder for scenario twelve was an employee of the marketing department at a tertiary hospital. One solicited respondent from a tertiary hospital's obstetrics department was advised not to participate by that hospital's Ethics and Compliance Officer.

Clinicians. A responding clinician to scenario twelve was a medical doctor who was a practicing obstetrician until closing this practice within the last year. This physician was currently employed by a consumer organization and also served on many administrative panels locally and nationally.

Consumer/Consumer Organizations. Two respondents answered as consumers to scenario twelve, they included an individual employed as a marketer for a pharmaceutical corporation and a patient

advisor for a cancer education network.

2.3.7.b. Domains

Information Use and Disclosure. The hospitals and physician group responding to the scenario indicated that direct marketing for the use of increasing revenue was not a current business practice; instead, these entities responded that they would utilize marketing as a means of improving quality of care. Although the use of PHI for marketing to increase revenue was not an identified business practice, the ability to do so did exist and consent from the patient would be obtained either through the admission paperwork or subsequently by the marketing department.

One respondent, an integrated delivery system, indicated that as a system with multiple facilities, they were established as a single covered entity under HIPAA. As a result, sharing information among their facilities did not require patient authorization.

Similar responses were obtained from hospitals responding to scenario twelve in that they shared information internally with other departments and they had registration forms targeted to marketing. The specificity of the registration form did include language, however, that allowed for patients to opt out of a mail list, implying that by not choosing to opt out they were automatically included. These hospitals also indicated that they did not sell patient information to outside vendors but instead let patients choose to register with vendors. This did not preempt vendors from including information and/or sample kits upon patient discharge.

One hospital responded that it transmitted identifiable data to a mail house to conduct patient-centered educational mailings or follow-up mailings to the patient after discharge.

A consumer responding to scenario twelve objected to the use and disclosure of information for marketing purposes. The

consumer viewed the practice as a negative practice and didn't feel it should exist.

The lack of variation that existed was due largely to what the activity was and whether the hospital viewed it as a marketing activity. Most of the purposes depicted in the scenarios did not constitute marketing according to the definition of marketing. [See 45 CFR § 164.501] Most facilities that responded to the Healthcare Marketing and Operations distinguished the purpose and intent for using patient information: 1. To inform, which is not marketing, and 2. To promote, which is marketing. The activity depicted in scenario eleven did not constitute marketing but two of the four business practices in scenario twelve, fund-raising and selling data, did require authorization. [See 45 CFR § 164.514 (f)(1) and § 164.508 (a)(3)]

2.3.7.c. Critical Observations

Scenario eleven was identified as not being applicable to the state of Utah. No entities were found to market in a fashion similar to that found in the scenario, in fact, the responding entities rarely marketed directly to individuals for identifiable health reasons. General brochures were a more common form of marketing in Utah as concerns were expressed about HIPAA and the use of PHI to generate revenue. In cases where covered entities did direct market, patient authorization was required (usually face-to-face).

One hospital system responding to scenario twelve reported having a business associate agreement with a mail house that specified the terms and limits of the contract for direct mailing. The hospital provided identifiable PHI on a compact disc or electronic file to the mail house that was specified for "one time use" and then destroyed. We found no selling of PHI to outside entities, although some hospitals did use the mail house as outlined above and others had an internal marketing department that sent information out. If the marketing was done internally the data was de-identified.

2.3.8. Bioterrorism

Scenario 13 Bioterrorism Event

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore this could be a possible Bioterrorism event. Further investigation confirms that this is a Bioterrorism event, and the State declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well informing the regional media to alert the public to symptoms and seek treatment if feel affected. The State also notifies the Federal Government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as they arise to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

2.3.8.a. Stakeholders

Physician Groups. The physicians responding to scenario thirteen were a semi-retired obstetrician, a general practitioner who served as a consultant for the state's quality improvement organization, and an emergency room physician at a tertiary hospital. With the exception of the emergency room physician, difficulty was noted with regards to identification of symptoms to anthrax exposure. Both the obstetrician and general practitioner stated that the difficulties in identifying anthrax exposure would result in loss of patient life and instead focus on secondary treatment precautions for other individuals exposed.

Law Enforcement. One individual representing the law enforcement stakeholder group was a detective that, similar to the emergency room physician, served on the variations work group. In this capacity, both detective and physician were able to identify

further variation and barriers to business practices identified in scenarios one, thirteen, and 13. Another respondent to scenario eight was Chief of Police for a town with a population of less than 15,000. The FBI also responded.

State Government (Public Health Departments). Individuals from the State Public Health Department's office of epidemiology and the state's bioterrorism unit responded to scenario thirteen. Respondents provided state government policy with regards to course of action in the case of suspected anthrax exposure.

Consumer/Consumer Organizations. No consumer or consumer group responded to Scenario 13

Other (Fire Department). One respondent was a firefighter in a district that is structured under the umbrella of Public Safety. The department employed 39 full-time fire fighter/EMT/paramedics and one part-time secretary and housed the Training and Operations Chief.

2.3.8.b. Domains

State Law Restrictions. All health care providers were required to report certain diseases to either the local or state public health department. HIPAA allows for reporting on PHI to public health in 45 CFR §164.512. In general, reporting of diseases was pursuant to The Communicable Disease Act found in Utah Code § 26-6. The provisions of Utah Code § 26-23b specifically applied to the reporting of information that indicated a bioterror event. HIPAA allows for public health reporting without patient authorization. It also allowed for both voluntary and mandatory disclosures to public health. [See 45 CFR §164.512]. HIPAA also allowed a covered entity to disclose PHI without authorization when necessary to avert a serious threat to health or safety, to disclose to federal officials involved in national security activities, and to correctional or law enforcement officials. (See 45 CFR § 164.512).

The Utah Health Code had two provisions dealing with disease reporting. The general reporting statute was Utah Code § 26-6-6: Duty to report individual suspected of having communicable disease; and § 26-23b-103: Mandatory reporting requirements - Contents of reports - Penalties. The Utah Department of Health rule that implemented these statutes is R386-702. Anthrax was listed among the reportable diseases.

Covered entities could share PHI with law enforcement as provided for in 45 CFR § 164.512(f) and (k). The HIPAA regulations did not apply to health information while it was held by an entity that was not a covered entity. Public health agencies were generally not governed by HIPAA in the use and disclosure of health information for their disease eradication efforts. However, state law limits how public health agencies could use personally identifiable health information. State law controlling public health agencies allowed them to share information with law enforcement but was limited to that necessary to protect the individual identified in the information and the peace officers and health care personnel involved. In this regard, it was more restrictive than the emergency disclosure provision of 42 CFR § 164.512(j).

2.3.8.c. Observations

There was consistent response from stakeholders regarding process and procedures for a suspected anthrax exposure. Physicians were well informed of their role in the required reporting process. The State Laboratory Response Network (LRN) was the hub department in our state, which sent critical information regarding anthrax cases. Variation existed in how information was released. The public health department was viewed as a one-way information street: they took information but did not readily give it. There were different levels of law enforcement involvement but the mechanisms of notification and the guidelines for sharing information were

unclear.

2.3.9. Employee Health

Scenario 14 Employee Health

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has exacerbated which is not work-related. The employee's condition necessitates a four-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than 2 days leave. The hospital Emergency Department has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information via email to the Human Resources department of the patient's employer.

2.3.9.a. Stakeholders

Hospitals. Responding to scenario 14 and representing the hospital stakeholder group was the privacy officer for an integrated delivery system. In addition, the HIPAA Director for a large research hospital also responded to this scenario. Finally, an emergency room physician at a large tertiary hospital responded.

Consumer/Consumer Organizations. A director of development at a local company that is self-insured responded on behalf of the consumers for this scenario. The company was one of the largest privately held companies in the state.

Other (Human Resources Department). The human resource department was from a small-to-mid sized company with 75 employees. The director of the human resources department responded to the scenario.

2.3.9.b. Domains

There were no reports of variation in the way hospitals handle "return to work" documents. We found no hospitals in the state that were willing to send a return to work document via email. Most have the patient deliver the document to their employer with some hospitals mailing or faxing the form. Consensus was found in this procedure. The only variation noted was in the capability of

facilities to email health information. Some hospitals reported an ability to process, encrypt and send PHI yet had not integrated this operating procedure or business practice. Other hospitals did not have technology to be able to send health information by email at all.

2.3.9.c. Observations

Hospitals responding to the scenario 14 reported that it was not common practice to transmit information via email. In particular, it was stated that a hospital would never 'cut and paste' information from the patient EHR system into a return to work form or use a printed page of a patient EHR for return to work purposes. Responding hospitals did not feel that this was in any way appropriate regarding this situation. The minimum necessary standard under HIPAA was, for the most part, a critical consideration given that "return to work" information requirements were general in nature.

2.3.10 Public Health

[Scenario 15 Public Health A](#)

A patient with active TB, still under treatment, has decided to move to a desert community that focuses on spiritual healing, without informing his physician. The TB is classified MDR (multi-drug resistant). The patient purchases a bus ticket - the bus ride will take a total of nine hours with two rest stops across several states. State A is made aware of the patient's intent two hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

[Scenario 16 Public Health B](#)

A newborn's screening test comes up positive for a state-mandated screening test and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response system. The state lab also enters the information in its registry, and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

[Scenario 17 Public Health C](#)

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. The person does have a primary provider, and is sent there for the medical care, and is referred to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement, and back to the shelter to verify that the person is in treatment. Someone claiming to be a relative of the homeless man requests information from the homeless shelter on all the health services the man has received. The staff at the homeless shelter is working to connect the homeless man with his relative.

2.3.10.a. Stakeholders

Clinicians. The clinician responding to scenario 17 was a licensed physician's assistant at a clinic that received funding from a combination of government, private foundation, and individual contributions. The clinic employed 29 full or part-time staff and administered primary health care services to homeless individuals and families in the Salt Lake City area.

Physician Groups. One physician that responded to scenario 17 was a family practitioner employed by a health center that was part of a larger integrated delivery system. The physician responding to scenarios 16 and 18 was a board certified general pediatrician employed by clinic that staffs 53 providers, approximately 250 employees and 18 different specialties. An IT Director employed by the largest group of independent physicians in the state of Utah, practicing in 15 specialties and currently having nine locations in Utah County, eight clinics in rural communities, and 500 employees responded to scenario 15.

Community Clinics and Health Centers. The respondent for scenario 17 was the executive director of a clinic that received funding from a combination of government, private foundation, and individual

contributions.

Laboratories. One of the respondents for scenario 16, representing a university-owned laboratory, was a physician serving as the medical director. The other respondent, representing the state-owned laboratory and further employed by a genetic collaborative center, provided current and ongoing education regarding newborn screening to practitioners and consumers and maintained quality in delivery of newborn screening services.

State Government (Public Health Departments). The manager of a data integration program that specialized in linking child health information from several programs which included: Vital Records (Birth and Death Certificates), USIIS (Utah Statewide Immunization Information System), Newborn Hearing Screening and Baby Watch/Early Intervention represented the state government public health department.

Law Enforcement. A detective and Chief of Police from a town with a population of less than 15,000 responded to scenario eight, thirteen and fifteen.

Consumer/Consumer Organizations. Consumer responses to scenario 15 and 17 were from an employee of the public health department and employees of a state-licensed substance abuse treatment center who had access to a consumer population deemed likely to be able to answer to the scenario with some authority.

2.3.10.b. Domains

State Law Restrictions. In the case of scenario 15, Utah required that all health care providers reported certain diseases to either the local or state public health department. HIPAA also allowed for reporting of PHI to public health without patient authorization. [See 45 CFR § 164.512] In general, reporting of diseases was pursuant to The Communicable Disease Act found in Utah Code § 26-6 that also allowed for Utah public health

agencies to disclose disease information to public health agencies in other states and to the Centers for Disease Control and Prevention. Utah Code § 26-6-27 permitted public health agencies to disclose personally identifiable communicable disease information to other public health agencies to prevent disease spread, however, Utah had no statute or rule that specifically required a common carrier, such as a bus company, to provide a manifest of the passengers to allow for rapid identification of individuals who may have been exposed to a communicable disease.

While HIPAA did not govern the disclosure of personally identifiable health information by public health agencies in the conduct of their efforts to interrupt the transmission of disease, A health care provider would likely be required to provide to local and state health departments relevant medical records regarding an individual who is subject to isolation or quarantine under the provisions of Utah Code Title 26, Chapter 6b. HIPAA allowed full disclosure of all records that state law requires to be disclosed. [See Utah Code § 26-6b-3.4 and Medical records — Privacy protections; 45 CFR § 164.512]

The protected health information held by the state lab in scenario 16 was not subject to HIPAA, but rather controlled by the Clinical Laboratory Improvement Amendments (42 CFR § 493), which required that the data went to the correct person. The state lab was part of the State Health Department, thus there was no barrier to transmitting the data to public health for follow-up. The newborn screening program was explicitly authorized under the public health statute UCA § 26-10-6 that did not allow for direct communication with the patient. The rules and statute directed that results be sent to the “medical home” or the practitioner caring for the child. The requirements for communicating the results to the provider were set forth in R398-1. There was no registry of Newborn Screening Data.

The Government Records Access and Management Act (GRAMA) did not govern who may access personally identifiable health information held by a public health agency as part of its public health efforts. The classification scheme under GRAMA specifically provided that records classified

under a different statute or by federal law were to be governed by that law. The method that the public may use to obtain access to public health records would still be governed by GRAMA. Protected health information held by a Utah governmental entity that was a covered entity subject to HIPAA was not governed by GRAMA.

2.3.10.c. Observations

As noted in previous scenarios, general precautions for transmitting patient health information were in practice. The public health department in scenario 15 did not disclose the medical condition (in this case tuberculosis) to law enforcement. As a result, law enforcement expressed dissatisfaction and concern as this policy seemingly put officers at risk. The public health perspective was that law enforcement should continually practice universal precautionary measures and, as such, risk is minimized.

Utah did not notify specialty care centers (as described in scenario sixteen) unless there were critical results as agreed upon with the specialist. Utah also did not have or use an Interactive Voice Response System or a registry for identified and confirmed cases of abnormal screening. Individually identified cases of phenylketonuria (PKU) and galactosemia were tracked through a Metabolic Clinic. Medical homes are notified of eligibility for this clinic upon diagnosis and the physician contacted the family of the child.

The state of Utah did not have county shelters as described in scenario seventeen. Further, it did not have a hospital-affiliated drug treatment clinic to serve the homeless. Utah's homeless were treated in social-based, not medical-based, facilities.

2.3.11 State Government Oversight

Scenario 18 Health Oversight Scenario

The Governor's office has expressed concern about compliance with immunization and lead screening requirements among low-income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education

are asked to share identifiable patient level health care data on an ongoing basis to determine if the children are getting the healthcare they need. This is not part of a legislative mandate. The Governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the Governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is not an existing contract with the state university for services of this nature.

2.3.11.a. Stakeholders

State Government (Public Health Departments). For the State Government Oversight Scenario, representing the state government public health department, was the manager of a data integration program that specialized in linking child health information from several programs which currently include: Vital Records (Birth and Death Certificates), USIIS (Utah Statewide Immunization Information System), Newborn Hearing Screening and Baby Watch/Early Intervention. Also responding for the state public health department with regards to scenario 18 were state program data stewards.

Medical and Public Health Schools that undertake Research. Representing a medical and public health school that undertook research was a licensed pediatrician with a university-affiliated practice that also served as assistant professor of pediatrics.

2.3.11.b. Domains

For Medicaid, a release of data to the university was part of HIPAA "TPO" if Medicaid required analysis of lead or immunizations. Authorization for the release was not required. (See 45 CFR § 164.506 (c)(1)). In this case, it was necessary for Medicaid to have a business associate agreement with the university. [See 45 CFR § 160.103(B)(ii); § 164.504]

The university was not allowed to re-disclose the information obtained through the business associate agreement (this could have been averted if re-disclosure was part of the contract). If the release of the data was not part of TPO, it would have required a HIPAA-compliant authorization signed by the participants or with proper IRB research approval. (See 45 CFR § 164.502; §164.512 (i)).

The data held by public health was not subject to HIPAA but was subject to the confidentiality requirements of U.C.A. § 26-1-17.5 that stated, "A record classified as confidential under this title shall remain confidential and be released according to the provisions of this title." The lead data was collected pursuant to R386-703 (1)(h) and was confidential pursuant to R 386-703-6(1). As such, it could not be released without a "written consent of the individual." (See U.C.A. § 26-6-27 (2)(a)).

Immunization data submission was voluntary and not comprehensive. The registry was governed by state rule. (See. R386-800-3). The participants in the scenario as "publicly funded programs" accessed the information through their own registration on the database. However, the right to use the data was limited. (See R386-900-06). Based on the wording of the scenario it was found to qualify as being "to confirm compliance with mandatory immunization requirements."

2.3.11.c. Observations

The Department of Health maintained the Utah State Immunization Information Systems (USIIS) that held records of children's immunizations. Approximately 130 of 350 provider offices had enrolled with user confidentiality to have access to USIIS. All office staff of participating providers was granted access to USIIS through an enrollment process. Access was renewed annually. Any office staff member that was terminated or released from employment was removed from having access. Only authorized health

care users had access to USIIS, this included researchers that had a legitimate research purpose and had IRB approval for a "look up only" basis. Utah also added lead poisoning to the injury surveillance and reporting system in 1990 per Utah Code R386 - 703 (Injury Reporting Rule).

Though Utah had the capacity to map and track this kind of information, this scenario raised the critical issue of data governance and sharing. As agencies and organizations worked together to effectively address issues similar to those portrayed in scenario 18, sharing information among agencies required more than a request from the governor. Multiple regulations and statutes, which govern how agencies and organization used and disclosed information, increased the difficulty of communicating. Common understanding, language, and guidelines were necessary to overcome the regulatory barriers that governed the ability to share and exchange information.

2.4 Summary of Critical Observations

Interoperability in healthcare systems has the potential to provide many benefits, even if defining interoperability can be a challenge. On more than one occasion our working groups posed the question of a definition for interoperability. As a general notion, we defined interoperability as "the ability of information systems to work together within and across boundaries to effectively exchange and use information." Promoting the use of interoperability was seen as a means of improving outcomes and reducing costs by improving efficiency. In addition, interoperability made possible a concerted effort to combat bioterrorism, the spread of disease, and other homeland security concerns.

The question to pose is "What access is needed for our stakeholders to operate in an interoperable healthcare environment?" During the course of our data collection, we found that Utah's healthcare system operated in both a paper *and* an electronic environment. As the state moves electronic information technology and e-Health forward, a comprehensive analysis is needed to understand the different requirements

regulating access to health information. Clear goals are needed to define Utah's e-Health system and the secure sharing of health information must be among the top priorities. Further dialogue is necessary among all participants involved in designing this interoperable system. This includes health insurers, physicians, hospitals, state health departments, local health departments, pharmacies, private industry, and others.

In considering interoperable health information exchange, it is also important to understand the stakeholder roles and how their applicable governance (or lack thereof) 'fit' into an interoperable system. Maximizing the benefits of interoperability and maintaining the individuals right to privacy and security require a clear working definition with achievable goals. Involved stakeholder entities must become part of the discussion as we move forward in the development of an interoperable healthcare system for Utah.

The reported absence of understanding with regards to regulatory requirements that govern individual agencies and partners (private or public) exchanging health information inhibit the exchange process. Furthermore, differing terminologies, standards, and concepts heightened barriers to interoperability, which in turn negatively impact secure information exchange in a timely manner. The confusion that existed within the stakeholder community with regards to sensitive health information exchange can also lead to the under-utilization of information and heighten fear of legal recourse.

While some stakeholders in the medical community work with a general understanding of HIPAA, the difficulty to exchange and transfer of information outside of HIPAA legislation increases significantly. In sum, when the environment is such that the exchange is outside of HIPAA alone, the exchange is as anything but seamless and barrier-free. Often the health information exchange process is a formal and cumbersome affair.

3.0 SOLUTIONS

The importance of interoperability in a 21st century global environment cannot be minimized. To avert public threats, bioterrorism, and to conduct public health surveillance requires that public health and law enforcement have and provide access to health information. Traditional public health surveillance and investigations were found to involve time-consuming manual reporting of cases to public health agencies and phone calls to healthcare providers for more detailed patient information. The value of exchanging existing health data electronically, and in a standardized format, provides a unique opportunity to leverage existing health data to better support public health functions of disease detection, monitoring, and real-time situational awareness.

The importance of privacy and security with regards to the health care consumer was at no time understated during the discussions of interoperability. Regardless of which workgroup was convened, the topic of consumer protection was voiced repeatedly. Ultimately, the SWG members determined that, prior to any discussion of implementation, a patient's 'Bill of Rights' should be established to ensure the consumer's ability to maintain a sense of ownership over their health information and establish a foundation to build consumer trust and confidence in e-Health. The core elements recommended in a consumer 'Bill of Rights' include the following:

Health care consumers should have the right to:

- Determine who is able to view their shared information;
- Revoke the right if they choose to do so;
- Request an audit of who has been viewing their information; and
- Be notified of any event that breaks these rights, such as breaking the glass, in emergency situations.

3.1 Summary of Key Findings from the Assessment of Variation

The privacy and security concerns identified in the Assessment of Variation report were a mix of technological, organizational, educational, and legal issues. This was likely due to the nature of the scenarios used to collect the business practice data. Although these four categories were delineated to further offer solutions, the categories came under the auspices of three general findings: an authorization to disclose, the transmission and transmission security of protected health information, and the applicability of relevant rules and statutes. Further critical observations were documented by scenario, by the VWG (see Appendix E).

Prioritizing findings were difficult in only two areas, that of authorization and transmission/transmission security. The applicability of relevant rules and statutes, while not to be disregarded, was significant on a lesser scale due to the vast amount of unwritten law in the state of Utah that guides business practice when compared to that which is implied under HIPAA and CFR 42 Part 2. Providers seek authorization from the patient to disclose and transmit patient health information, typically via facsimile, to other providers involved in the patient's treatment. Facsimile security protocols were found to vary in significantly. PHI was reportedly discussed over the phone between providers without patient authorization to a source that had no other formal verification than a oral confirmation from the voice on the phone. As a result, the items below are ranked in no particular order with the exception of rules and statutes.

Authorization to disclose. Disclosing patient information without authorization was found to be allowable under HIPAA for "treatment, payment and healthcare operations." However, most providers chose to get patient authorization prior to disclosing health information. This did not appear to be an education issue, as providers generally understood this HIPAA provision and what constituted an allowable

disclosure. For many health care providers, the garnering of patient consent/authorization was 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 refused to release the patient information without patient authorization, even though it was allowed under HIPAA.

Transmission and transmission security of Protected Health Information (PHI). There was 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 had 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 had the ability to use encrypted email but this method was not yet widely used and accepted. Some facilities reported having policies in place that prohibited 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 were employed with radiology films (e.g. x-rays), especially among large facilities. Mammography films were 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 used these methods. Instead, films were 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 was not a covered entity under HIPAA nor was Public Health or the State Public Health Laboratories. Although substance treatment facilities were covered entities, they also complied with 42 CFR Part 2, a federal regulation that heightened protection for treatment records. Primary care providers reported that they disregarded treatment facilities' records because the associated difficulties in accessing them. HIPAA and 42 CFR Part 2 did not align in a manner that was conducive to health information exchange.

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.

3.2. Effective Practices

As the VWG was instructed to classify business practices as barrier, aid, or neutral "without judgment," most business practices were classified as a barrier. The identification of "effective" business practices did not occur until the SWG had convened and utilized a decision-making process to achieve consensus.

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 reconsider CFR 42 Part 2, in light of the changing environment and not as a result of the law's stringent approach to the disclosure of substance abuse information because all personal health information is worthy of high standards for security, protection and equal treatment. However, it was written prior to the use of electronic media for health information access, viewing and storage.

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 theo-

retically covers the entities not once, but twice. In addition, this practice, although not necessary under HIPAA, provides protection to both the entity and the consumer further illustrated 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).

Overall, the SWG determined that the need to maintain health care consumer privacy and security outweighed any benefits of interoperability or the free exchange of information. This was further found to be an overriding determinant rather than just occurring in relatively few scenarios. It was also determined that, due to the expertise and authority of SWG members, the business practice data were often disagreed with and negated as being hypothetical or as occurring outside the realm of the 'real world.' For example, the stakeholder responding to scenario five detailed a business practice that enabled a payer to have electronic access to a clinician's EHR system. This practice, as determined by the SWG chair, would not take place, as payers would limit themselves to a minimum amount of information. This practice would protect both the payer and practitioner from inadvertent use of consumer PHI.

3.3. Identification of Variations Not Being Addressed by the SWG

All business practices identified by the VWG were addressed by the SWG and grouped according to practice being a barrier, neutral, or an aid. If the practice

was found to be effective, if it did not violate the consumer's rights regarding privacy and security, and if it was electronic or could not be made electronic, the SWG did not deliberate further. As a result, no variations identified by the VWG went unreported.

4.0 ANALYSIS OF SOLUTIONS

Following the VWG analysis of the 18 scenarios and the accompanying identification of 144 business practices, the LWG (see Appendix D) convened, per RTI instruction, to determine which business practices identified by stakeholders had state legal drivers. Sponsored by the Utah Attorney General's Office, and chaired by Lyle Odendahl, JD⁹, the LWG found that no statutory conflicts existed, however, Utah privacy and common tort law does drive organizational and business practice that prohibit HIE according to HIPAA. Furthermore, variation existed as to knowledge regarding the exchange or disclosure of protected health information (PHI) between covered and non-covered entities. To illustrate, it was found that law enforcement would often request PHI, and feel they had a right to receive said PHI, due to the fact that they were not a covered entity (i.e. health plan, medical clearinghouse, health care provider, and prescription drug card sponsor) while covered entities were not allowed to disclose PHI as HIPAA prevented them from doing so. [See 45 CFR 160.103 for the few statutory exemptions]

It was further decided that the solutions categories fall into one or more of four domains: technical, administrative, educational, and legislative. As such, it was important to reconsider the business practices identified as barriers as falling into one or more of these four domains as well.

5.0 STATE SOLUTION IDENTIFICATION AND SELECTION PROCESS

5.1. The State Solutions Workgroup

Sponsored by UHIN and chaired by Linn Baker (Executive Director of Public Employees Health Plan and member of the UHIN Executive Committee), the Solutions Workgroup (see Appendix D) examined those business practices identified by the VWG and defined, via decision tree (see Appendix F), which business practices served as barriers to the electronic exchange of PHI. The SWG further objectively identified which business practices were an aid or neutral to the electronic exchange of PHI and if the business practices protected the health care consumer's privacy and security. If the business practice was determined to be a barrier, or if the health care consumer's privacy and security was not deemed protected, the SWG sought to determine a solution.

5.2 Identifying Solutions

To further identify and propose solutions, the SWG further delineated the three key findings of the VWG (authorization to disclose, transmission and transmission security of PHI, and applicability of relevant rules and statutes) into four solution categories as such:

Technological:

- Transmission of PHI. The method of choice for transmission of PHI in the state of Utah was the facsimile although several stakeholder entities also reported that the use of government mail and/or courier was an option. It was also reported that PHI would be released to the health care consumer, or a representative of the health care consumer, with proper identification. This was most common with regards to radiological images.
- Transmission Security of PHI. The consensus among stakeholders was that the transmission of PHI via email, encrypted or otherwise, was not good practice due to privacy and security concerns. Security precautions taken when faxing PHI also varied from the practice(s) of calling an entity prior to and following the transmission of PHI as well as

maintaining a signed log. Overall, privacy and security concerns were of major importance to stakeholders and the practice of faxing PHI was identified as being the most desirable under current conditions.

- Authentication/Verification. It was common practice (in a physician office or hospital setting) to regularly disclose health information over the phone to other health care professionals as long as there was a common level of understanding and/or trust. While a credentials database existed within the realm of UHIN, and the Division of Occupational and Professional Licensing maintained some licensing information, they were by no means considered all-inclusive.
- Locating PHI. Little variation was found among stakeholders with regards to locating PHI for treatment, payment, or healthcare operations. Most stakeholders responding sought to locate the whereabouts of PHI directly from the healthcare consumer, or consumer representative, when possible. It was noted that in emergency situations this was difficult, if not impossible, when the health care consumer was incoherent or incapacitated.
- Accessing PHI. Interoperability and access to PHI among stakeholders was often made more difficult when the stakeholders involved were deemed competitors. In instances where a stakeholder knew the location of PHI, access was not likely to be granted and instead a request would be issued. This served as an example of an entity receiving PHI as a result of a 'push' from another entity rather than a 'pull.'

Administrative:

- Authorization to Disclose. Disclosing patient information without patient authorization was allowable for “treatment, payment and healthcare operations” under HIPAA; however most providers chose to get patient authorization prior to disclosing health information. This was further found to be desirable practice and not likely to change as the majority of individuals felt the added precaution was also added protection against legal recourse and, as a result, served as administrative policy. Authorization was further confounded when information reached the state level, as the Department of Health is not bound by regulation to disclose PHI. This was found to be a matter of contention between providers and law enforcement with regards to safety of first responders.
- Transmission of PHI. Variation was not found in the transmission policies and practices among stakeholder entities as fax was most common and administrative policy forbid email transmission.
- Transmission Security of PHI. The majority of stakeholders reported transmitting PHI by using a cover sheet that displayed their identifying letterhead. The majority of substance abuse clinics responding indicated that they would also notify the receiving entity, by telephone, that a fax was being transmitted and then would follow-up with a phone call to confirm.
- Allowing Access to PHI. Access to PHI was often granted based on the nature of the PHI involved and the purpose of the request. It was found to be common practice among stakeholders to establish a business agreement

prior to allowing access to PHI unless a conflict of interest was identified (e.g. competing entities), in which case PHI would be disclosed rather than allowed by access. It was also found that an electronic exchange of PHI was most often done by ‘push’ rather than ‘pull’ when following administrative protocol. Further barriers to the exchange of information were determined to be between non-competing entities within the Department of Health. Although administrative policy did allow for limited sharing, a culture existed that limited sharing as a result of perceived ‘ownership’ of PHI.

Legislative:

- Applicability of Relevant Rules and Statutes. Difficulty in exchanging health information increased when different rules and statutes applied to entities involved in the exchange of health information. Law enforcement is not a covered entity under HIPAA, nor is Public Health or State Public Health Laboratories. Although substance abuse treatment facilities are covered entities, they also complied with 42 CFR Part 2, a federal regulation that heightened protection for treatment records.

Educational:

- Privacy and Security of PHI. Health care consumers in the state of Utah were found to be uninformed as to their rights regarding the usages of personal or protected health information. Many consumers received their information from non-news television programs or non-scholarly media outlets and, as a result, held beliefs that their personal health information was either more protected or, conversely, less protected than it actually was.
- Benefits to HIE. Consumers interviewed had very little knowledge regarding the benefits to interoperability.

- Providing education regarding risks and realities of communicable diseases. A chasm was identified between law enforcement first-responder personnel and medical personnel with regards to the dangers (both perceived and warranted) of communicable disease for first responders.

5.3 Inappropriate Scenarios or Exchanges

It was further decided that seven of the scenarios, some previously identified by the VWG, were irrelevant to the state of Utah with regards to information exchange: *Scenario Five – Payment*, *Scenario Six – RHIO*, *Scenario Eleven – Healthcare Operations and Marketing A*, *Scenario Twelve – Healthcare Operations and Marketing B*, *Scenario Fourteen – Employee Health*, *Scenario Seventeen – Public Health C*, and *Scenario Eighteen – Health Oversight*. Although these scenarios were not found to be applicable to HIE as it occurs in Utah, stakeholders felt that theoretical exchanges were worth mentioning if they were found to be a possibility.

Scenario Five – Payment. This scenario was identified as being unlikely in the state of Utah as stakeholders were not aware of any Health Payer that would request access to a health provider's EHR to approve/authorize inpatient encounters. That being said, both payers and clinicians were in agreement with the main concept that only the "minimum necessary" under HIPAA would be given to the payer.

Scenario Six – RHIO. Monitoring of patient or physician data would not happen in Utah as UHIN is a gateway or information highway where information is exchanged between different organizations and, as such, it did not request or permanently store data. UHIN instead functioned like the post office in getting information routed from the sender to the intended receiver and did not perform quality measurements on its members' data. Should members want to exchange/submit patient information from one organization to another, UHIN's standards committee could

charter a subcommittee to develop a community-standardized message.

Scenario Eleven – Healthcare Operations and Marketing A. Scenario 11 was identified as not being applicable to the state of Utah. No entities were found to market in a fashion similar to that found in the scenario, in fact, the responding entities rarely market directly to individuals for identifiable health reasons. General brochures are a more common form of marketing in Utah as concerns were expressed about HIPAA and the use of PHI to generate revenue. In cases where covered entities direct market, patient authorization would be required (usually face-to-face).

Scenario Twelve. Healthcare Operations and Marketing B: Further discrepancy was noted with regards to scenario 12 as one hospital system responding reported that a business associate agreement with a mail house existed that specified the terms and limits of the contract for direct mailing. The hospital provided identifiable PHI on a compact disc or electronic file to the mail house that is specified for "one time use" and then destroyed. We found no selling of PHI to outside entities, although some hospitals use the mail house as outlined above and others have an internal marketing department that sends information out. If the marketing is done internally the data are de-identified.

Scenario Fourteen – Employee Health. Hospitals responding to scenario 14 reported that it is not common practice to transmit information via email. In particular, it would never be the situation that a hospital would cut and paste information from the patient EHR system into a return to work form or use a printed page of a patient EHR for return to work purposes. Responding hospitals did not feel this was appropriate in this particular situation. The minimum necessary standard under HIPAA was, for most, a critical consideration given that "return to work" information requirements are general in nature. The only variation noted was in the capability of facilities to email health information. Some hospitals have good

processes for encrypting and sending protected health information yet have not integrated this in their processes. Other hospitals do not have technology to be able to send health information by email at all.

Scenario Seventeen – Public Health C.
The state of Utah does not have county shelters as described in scenario seventeen nor does it have hospital-affiliated drug treatment clinics that serve the homeless. Its homeless are treated in social-based, not medical based, facilities. It is also rare that a homeless person would have a primary care provider.

Scenario Eighteen – Health Oversight.
The Health Oversight scenario details a governor's request to establish a database for childhood immunizations and blood lead to determine if individuals seek treatment by 'migrating' between states. Though Utah has the capacity to map and currently tracks this kind of information, this scenario raises the critical issue of data governance and sharing. As agencies and organizations work together to effectively address issues similar to those portrayed in scenario 18, sharing information among agencies may require more than a request from the governor (such as an executive order). Multiple regulations and statutes, which govern how agencies and organization use and disclose information, increase the difficulty of communicating. Common, understanding, language, and guidelines are necessary to overcome the regulatory barriers that govern their ability to share and exchange information.

The elimination of these seven scenarios for consideration left the remaining eleven to be categorized into the four solutions categories (technical, administrative, legislative, and educational).

5.4 Vetting, Evaluating and Prioritizing Solutions

As the chair of the SWG was Director of Utah's Public Employee Health Program and a member of UHIN's Executive Committee, one of the SWG members

was the Assistant to the Executive Director of UHIN, and yet another was in the process of securing funding for an independent banking model, it was determined (although unspoken) that a technical solution category would be prioritized. UHIN's history in the state of Utah has been well documented and SWG members determined that there was no need to contemplate a technical solution that did not directly involve UHIN. As a result, the remaining solutions categories were often (if inadvertently) incorporated into UHIN's structure. For example, some Administrative Solutions (transmission of PHI, transmission security of PHI, and allowing access to PHI) were determined applicable to UHIN's proposed structure as the transmission, security, and access could be accommodated for. The remaining two categories (Legislative and Education) were determined to be, respectively, national and grass roots issues as Legislative Solutions involved the revision of HIPAA and the Education Solutions were primarily intra-agency.

5.5 Organizing and Presenting Solutions

Following SWG review of each business practice and the subsequent classification as barrier, neutral and aid, it was further found that scenario business practices fell into multiple solutions categories and, as such, the SWG re-categorized scenario business practices according to applicable solution categories:

Technological:

· *Scenario One Patient Care A:*

Transmission of PHI In emergency situations, hospitals and physicians disclosed information via facsimile transmission or by telephone if the requesting entity identified themselves as a physician or an individual acting on behalf of a physician. In such instances it was found to be common business practice to follow up a telephone request with a fax stating the request in order to document the information exchange in the patient chart. In most non-emergent situations the entity receiving a request for PHI requested

that a consent form, with the patient's signature or a patient representative signature, be sent prior to PHI disclosure.

Authentication/Verification While a level of trust did exist between care providers when exchanging PHI, one stakeholder conveyed that the practice of authenticating and verifying a requesting entity was done via the Internet. Another stakeholder responded that this was not the norm as an exchange of PHI was commonplace and, at best, a verbal request was followed up with a fax request that was placed in the patient's chart. While a credentials database exists, and The Division of Occupational and Professional Licensing maintains some licensing information, they are by no means considered all-inclusive.

Locating PHI In an emergency situation, a physician made every effort to locate a patient's medical information with a patient's assistance and authorization (or family member's assistance and authorization) if the patient was coherent or if a family member was present. In more complicated situations, this information gathering required locating PHI from internal and/or external sources. Internally, this entailed searching the hospital data banks to determine if the patient had previously been seen there. Externally, this information gathering was often not possible if the patient's medical history was verbally unattainable from the patient or a patient representative. Regardless, locating PHI was seen as being imperative to gain a full history of the patient and treat as appropriate while decreasing the chance for medical error.

Accessing PHI Electronic external access to PHI was not an option in Utah as no agreements for access into individually held EMR databases

were in place between providers. It was further noted that there was an identified conflict between one tertiary hospital's inpatient EMR system and that same hospital's outpatient EMR system. To further elaborate, a physician performing inpatient surgery and then seeing the same patient for a follow-up exam in an outpatient setting, electronic access of the inpatient PHI would not be possible and a record request would be needed.

The release of patient information across state lines was not found to be a factor with regards to the exchange of patient information. It is unclear what the requirements would be from neighboring states to disclose patient information. Hospitals responding within the state of Utah report that in an emergency, the information request would be fulfilled following authentication of the requestor via fax of requesting entity's letterhead. If not an emergency situation the practice is to have patient authorization to disclose.

· *Scenario Two Patient Care B:*

Transmission Security of PHI

While the added precautions and protections afforded to substance abuse information will be covered in-depth in the legislative key findings, it stands to say that, as a result of CFR 42 Part 2, substance abuse information is treated with more stringent privacy and security precautions than other PHI. An interesting note however was that the transmission of substance abuse information is done via fax, similar to any and all other categories of PHI, regardless of added legislation. An extra precaution that select, but not all, stakeholders take when transmitting substance abuse information was that a phone call

is made to notify that the information is being sent and then again to confirm that the information was received by the appropriate party.

Authentication/Verification While substance abuse information is protected under CFR 42 Part 2, no added precaution of authentication or verification occurred other than would take place with other forms of PHI. Stakeholders were found to agree that the health care community in Utah (with regards to substance abuse information) is small enough that most all involved experience some degree of familiarity that renders any authentication or verification obsolete.

- *Scenario Three Patient Care C:*
Transmission of PHI Most information transmitted to and from long-term care facilities was reported to occur by by fax with no additional security being in place.

Allowing Access to PHI There was variation among long-term care facilities' practices for granting physicians temporary access to their facility and records system but facilities have procedures in place should temporary access be necessary under such situations. The sharing of patient information differed from entity to entity with some requiring that a business associate agreement be in place and others indicating such agreements are not necessary between providers involved in the treatment of a patient.

- *Scenario Four Patient Care D:*
Transmission of PHI The majority of mammograms done in Utah were reportedly film; this was the case in both rural and urban facilities. One integrated delivery

system currently reported the use of digital images for mammography and a second plans to transfer to digital within the next two years. However, even at the integrated delivery system that uses digital, the images are printed in hard copy for the physicians as most institutions and physicians are not comfortable with digital. These films were transmitted or exchanged by mail, courier, or the patient with signed patient release. This transmission were contrary to recent technological advances that would allow, with proper bandwidth, the transmission of digital images for physician diagnosis. Moreover, with the Picture Archival Communication System (PACS) becoming more prevalent with regards to digital images of mammograms, it was observed that the variation in transmission protocol was more the result of physician comfort level with reading digital images, as it was an inability to transmit.

- *Scenario Sixteen Public Health B:*
Transmission of PHI Utah does not have an Interactive Voice Response System or a registry for identified and confirmed cases of abnormal screening. Individually identified cases of phenylketonuria (PKU) and galactosemia patients can be tracked through a Metabolic Clinic however. The lack of an Interactive Voice Response System indicates that a need for electronic interoperability exists as a paper system is currently in place.

Administrative:

- *Scenario Three Patient Care C:*
Transmission of PHI Most information transmitted to and from long-term care facilities was reportedly done by fax as an administrative rule of thumb.

Transmission Security of PHI It was further noted that the majority of long-term care facilities have established the fax as a transmission protocol for

security reasons as email is not a trusted means of transmission.

Allowing Access to PHI The sharing of patient information differed from entity to entity with some requiring that a business associate agreement be in place and others indicating such agreements are not necessary between providers involved in the treatment of a patient. Long-term care facilities required a login and password for all staff with access granted on a “need to know” basis. They do not have sharable passwords. The long-term care facility can grant a health care provider access to patient records when appropriate. The decision to grant temporary access to the patient record via the electronic system was at the discretion of the long-term care facility. Long-term care facilities operating electronic medical records required technical safeguards including unique user identification and procedures for accessing electronic PHI in an emergency. This would be true even if access were temporary.

- *Scenario Thirteen Bioterrorism:*
Authorization to Disclose State Health Code regulates public health agencies use and disclosure of personally identifiable health information. Public health agencies permits sharing of information with law enforcement but is limited to that necessary to protect the individual. Information sharing for safety and protection purposes is not mutually defined, however, systems and procedures are established. The degree of sharing is at the discretion of public health officials.
- *Scenario Fifteen Public Health A:*
Allowing Access to PHI Although intra-agency access was reported as allowable within the state Department of Health, little exchange was found to exist in actuality. Conversation and a need for a

solution to this identified practice occurred within the SWG as a member was the data steward for tuberculosis data. It was further identified that a request for funding from the state was in place that would allow for an updated integrated system allowing for great control and access to pertinent public health information that could be utilized to identify public health threats.

Legislative:

- *Scenario Two Patient Care B:*
Applicability of Relevant Rules and Statutes PHI containing a history of substance abuse is shared, following patient authorization according to the specifics of 42 CFR, Part 2, which details what information is to be exchanged, between what parties, and for what period of time. This “minimum information sent” was described by a physician’s assistant as having “little utility” and therefore was disregarded in favor of obtaining the patient’s history of substance abuse from the patient. This notion of “little utility” was again voiced by a general care practitioner who indicated that a specialist would determine what information was needed and initiate the request for PHI with the substance abuse patient in the specialist’s office. The type and amount of information disclosed by the substance abuse treatment facility is limited to that which is necessary and for which the patient has given consent. 42 CFR Part 2 contains a consent-driven disclosure mechanism. HIPAA contains a minimum necessary-driven disclosure mechanism. The Privacy Rule allows for communications within programs on a “need to know” basis. 42 CFR Part 2 requires that the communication of information

within the program (or to an entity with direct administrative control over the program) be limited to those persons who have a need for the information in connection with their duties that arise out of the provision of diagnosis, treatment or referral for treatment of alcohol or drug abuse (see 42 CFR § 2.12). The type and amount of information disclosed by a Substance Abuse Treatment Facility is limited to that which is necessary and for which the patient has given consent. 42 CFR Part 2 does not discuss transmission of PHI.

Educational:

Scenario Eight Law Enforcement:

Privacy and Security of PHI Laws and regulations that govern healthcare entities and law enforcement are different as is the intent from which those laws are based. Healthcare entities, with regard to exchange of patient information, focus on the protection of that patient's privacy. Law enforcement, though not disregarding the individual's right to privacy, must focus on the protection of the broader community. The VWG did determine that, while a difference did exist regarding the understanding of what it meant to be a 'covered entity,' the consumers responding lack a true understanding of what rights (or lack thereof) existed with regards to PHI.

To clarify, while law enforcement demonstrated a tendency to believe that, since they were not a 'covered entity,' they had a right to PHI, providers would not disclose said PHI, as they were a 'covered entity.' The consumer, on the other hand, felt as though they controlled who had access to their PHI and were ignorant

with regards to provisions allowing for the exchange of PHI for 'treatment, payment, and healthcare operations.'

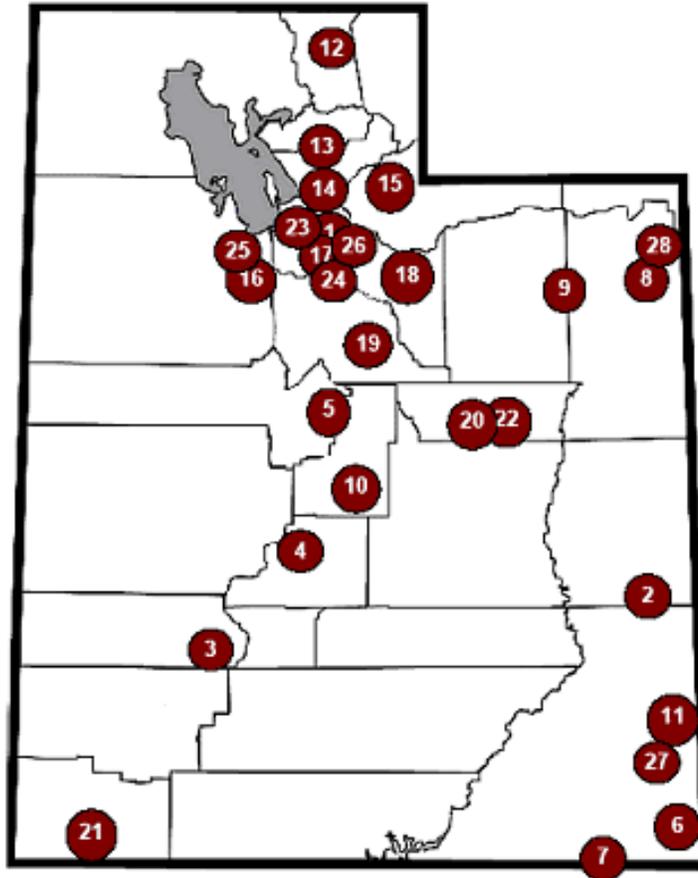
Scenario Fifteen Public Health A:

Providing education regarding risks and realities of communicable diseases As noted in previous scenarios, general precautions for transmitting patient health information are in place. The public health department in Scenario 15 is cautious to not disclose a medical condition (in this case tuberculosis) to law enforcement. As a result, the law enforcement expressed dissatisfaction and concern as this policy can put officers at a disadvantage. The public health perspective is to advise law enforcement to take precautionary measures regardless. However, it is common practice for law enforcement to take into account relevant information and enact precautionary measures accordingly. Law enforcement stakeholders also did not express relief when told there was "greater risk of being in a car accident than contracting TB while transporting a patient with the windows rolled down."

5.6 Determination of Feasibility

Given the nature of the solution categories and the expertise of the SWG members, feasibility was extensively discussed. A licensed physician with a graduate degree in medical informatics served as a champion for the independent banking model, the director of a major payer and member of UHIN's executive committee served as the champion for UHIN's central role in the technical solutions, and UHIN's assistant executive director served on the SWG led the solutions discussion of feasibility to examine possible flaws and obstacles. It was in this manner that all solutions forwarded to the Implementation Planning Work Group (IPWG) were evaluated. Feasibility of technical solutions are dependent on UHIN's Executive Boards willingness to adopt and incorporate strategically into UHIN's long-term workplan.

Figure 1. Utah Telehealth Network Sites.



Site UTN Network Members

- | | |
|--|---|
| 1 University of Utah, SLC | 18 Wasatch County Health Department, Heber City |
| 2 Allen Memorial Hospital, Moab | 19 Utah County Health Department, Provo |
| 3 Beaver Valley Hospital, Beaver | 20 Southeastern Utah Health Department, Price |
| 4 Central Utah Health Department, Richfield | 21 Southwest Utah Health Department, St. George |
| 5 Central Valley Medical Center, Nephi | 22 Castleview Hospital, Price (no videoconferencing) |
| 6 Montezuma Creek Community Health Center, M.C. | 23 UDOH - Cannon Building, SLC |
| 7 Monument Valley Health Center, M.V. | 24 Elaine Skalabrin, M.D. Residence (Telestroke Emergency), Sandy |
| 8 TriCounty Health Department, Vernal | 25 Mountain West Medical Center, Tooele |
| 9 Uintah Basin Medical Center, Roosevelt | 26 Utah Hospital & Health System Association, SLC |
| 10 Gunnison Valley Hospital, Gunnison | 27 UNHS Blanding Family Practice, Blanding |
| 11 San Juan Hospital, Monticello | 28 Basin Clinic, Vernal |
| 12 Bear River Health Department, Logan | |
| 13 Weber-Morgan Health Department, Ogden | |
| 14 Davis County Health Department, Farmington | |
| 15 Summit County Health Department, Coalville | |
| 16 Tooele County Health Department, Tooele | |
| 17 Salt Lake City-County Health Department, Murray | |

6.0 Analysis of Proposed Solutions

Following a review and reconsideration of the VWG findings, those business practices identified as barriers to the secure exchange of PHI were further delegated by the SWG to an applicable solution category. Current and planned electronic projects were incorporated into solution results where possible and where deemed appropriate by the SWG. The identified solutions represent the SWG effort to address identified challenges to the electronic exchange of health information while maintaining the security and privacy of that information. They were 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. Scenarios in which solutions categories were heavily identified are placed behind the identified barrier in parentheses.

6.1 Solutions to Variations in Organization Business Practices and Policies

Technological:

Identified Barrier. An inability to transmit PHI via secure methods whether by portal or other technology to all areas of the state.

[Transmission of PHI: Scenario One Patient Care A, Scenario Three Patient Care C, Scenario Four Patient Care D, Scenario Sixteen Public health B].

Proposed Solution: To continue to establish an electronic 'pipeline' that will include rural as well as urban areas. Connectivity would not be established by UHIN, but via Utah Telehealth Network. Paid membership to UHIN will then allow for transfer of administrative data with providers and payers from all areas of the state. The secure transfer of clinical data would result pending the success of pilot trials currently underway at UHIN.

General context: Rural health care facilities have relationships with distant healthcare providers and payers with which they need to exchange clinical and administrative data. Many rural areas of the state were found to have limited infrastructure to support high-speed networks. The Utah Telehealth Network has worked closely with telecommunications companies, the University of Utah, Utah Healthnet, 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. Discussion also took place with regards to the expansion of communication towers that would allow for wireless communication in a secured environment.

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 were 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 allowed 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). Also UHIN is involved in pilot exchanges of clinical data.

Identified Barrier. Inability to properly ensure transmission security of PHI via facsimile and/or paper transmission and a lack of trust regarding the privacy and security of electronic exchange.

[Transmission Security: Scenario Two Patient Care B].

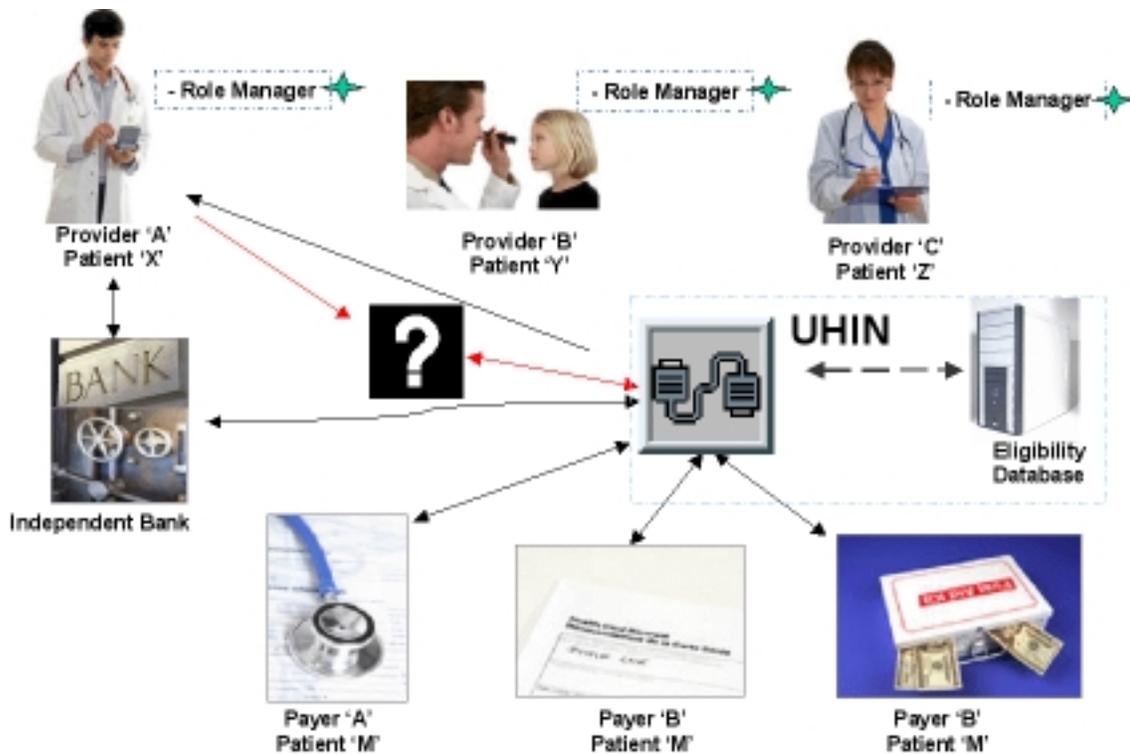
Proposed Solution: To utilize UHIN for secure clinical exchange as a plausible solution. This is due to the fact that the exchange of administrative claim data was already in place. Accompanying the proposed solution is expanding interoperability state-wide, this proposed solution could readily be implemented with the assurance to providers that clinical data would operate under the same auspices currently in place and the transmission of data via portal could provide more security than that which takes place with a fax transmission.

General context: Although a SWG member attempted to initiate discussion regarding facsimile protocol that could be immediately incorporated, the majority of SWG members chose instead to focus on the future practice of interoperability and transmission by methods other than fax. The major consumer

concern regarding interoperability was the concern of transmission security.

Extent to which solution is in use: The UHIN Security Education Tool (USET) was created to assist small healthcare providers in their efforts to understand and develop reasonable and appropriate security policies for exchanging administrative claim data in accordance with HIPAA guidelines. Although using USET does not guarantee any surety of HIPAA security compliance, it does provide a template for establishing protocol regarding secure electronic exchange. UHIN also utilized public key infrastructure (PKI) at the organizational level that enabled computer users to be authenticated to each other, and to further use the information in identity certificates to encrypt and decrypt messages travelling to and from. Due to the fact that administrative claim data is currently being ex-

Figure 2. Short-term concept model for state connectivity.



changed in a secure electronic environment, UHIN was determined to be a reasonable vehicle for the secure transmission of electronic claim data for participating members pending successful trial exchange.

Identified Barrier. Authentication/verification of provider utilizing electronic portals for the exchange of PHI.

[Authentication/Verification: Scenario One Patient Care A, Scenario Two Patient Care B].

Proposed Solution: Establish a system or standard protocol for authentication and verification of provider authority to access PHI. A system similar to this was found to be operated by UHIN to establish an 'end user' or 'super user' that takes responsibility for the security of individuals or entities transmitting and/or receiving PHI electronically. The 'super user' is established through an authentication process by UHIN following a site visit. Once the 'super user' is established, that entity would grant authorization to allow access to the UHIN portal. This would alleviate UHIN from any authentication/verification of users and places responsibility on the 'super user' to maintain a credible system whereby inappropriate access is prevented.

General context: Authentication was determined essential to prevent the inadvertent or inappropriate release of information. It was further found that all information should be accessible only on a need-to-know basis. Ensuring that information was only released after the identity of the requestor was confirmed was found to be critical. Identified security policies typically relied on a request faxed on letterhead.

Extent to which solution is in use: UHIN policy was to visit each participating member to authenticate the member location and designate a site-specific role manager. The role manager was then responsible for verifying physicians and providers at their location.

Identified Barrier. Locating PHI electronically and in 'real time.'

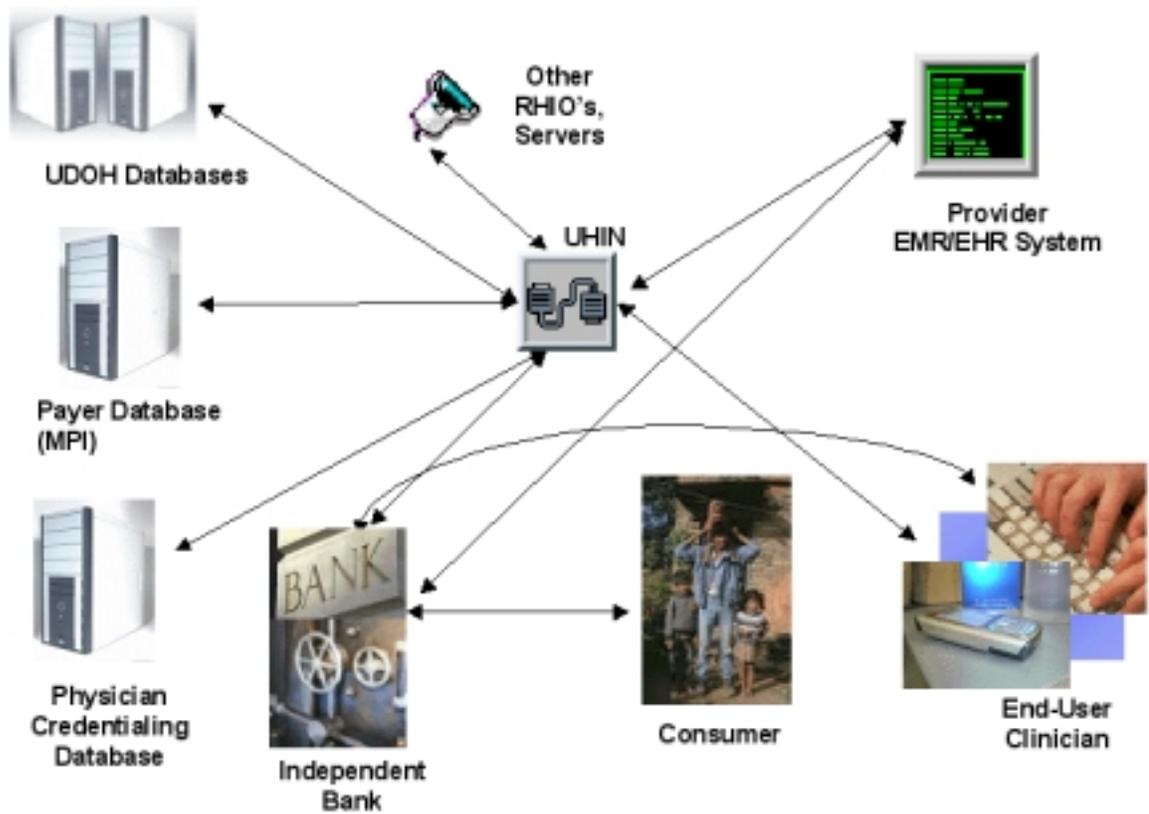
[Locating PHI: Scenario One Patient Care A].

Proposed 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. Furthermore, 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. It was also suggested that the common identifier would remain the same when an individual changed plans. This solution is further identified as not affecting the uninsured and it was hoped that Medicare cooperates in accepting the common identifier format.

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. 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. (See Figure 2).

Extent to which solution is in use: Policies are in place for limited sharing only. However, no common identifier exists. It was found that, due to UHIN's unique nature, this proposed solution differed from many other states participating in this study. The notion of a common identifier or Master Patient Index (MPI) has been contested at the national level for fear of privacy and security breaches. The proposed solution by UHIN is more similar to an Enterprise Master Patient Index (EMPI) due to the fact that the number would remain within the realm of UHIN and the state of Utah. This solution was further championed by the SWG

Figure 3. Long-term concept model for state-wide connectivity.



chair as a result of UHIN's executive committee being largely payer-based and willing to work in concert with one another. 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. One possible solution to this was identified as being private industry developing consumer-driven health data banks. Although it was stated by a UHIN representative that UHIN did not wish to serve as a record locator or information repository, it was found conceivable that in a proposed long-term solution UHIN could allow for the transmission of PHI from an identified entity to a requesting entity. (See Figure 3).

Identified Barrier. Accessing PHI. [Scenario One Patient Care A]

Proposed Solution: As most provider entities in the state of Utah are deemed competitors, a reluctance exists to allow for a 'crosswalk' enabling access to a healthcare system's data repository. The solution offers a long-term resolution where by UHIN would serve as the trusted entity responsible for locating and transmitting PHI between entities. [See Figure 3]

General context: Not applicable.

Extent to which solution is in use: Not applicable.

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 towards 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

Figure 4. Emergency response reporting system, NEMIS/POLARIS.

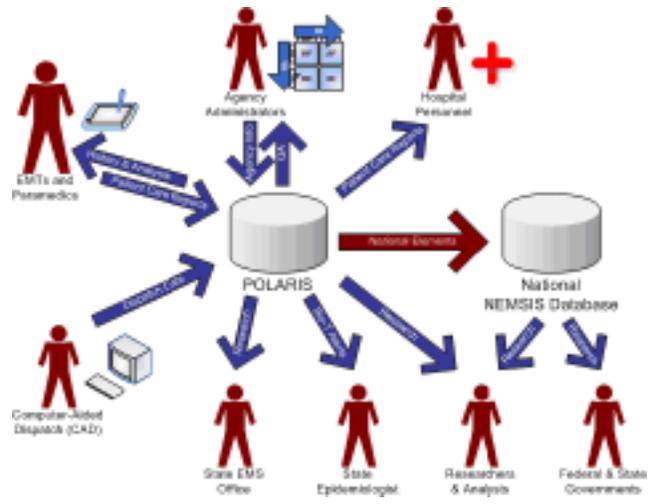
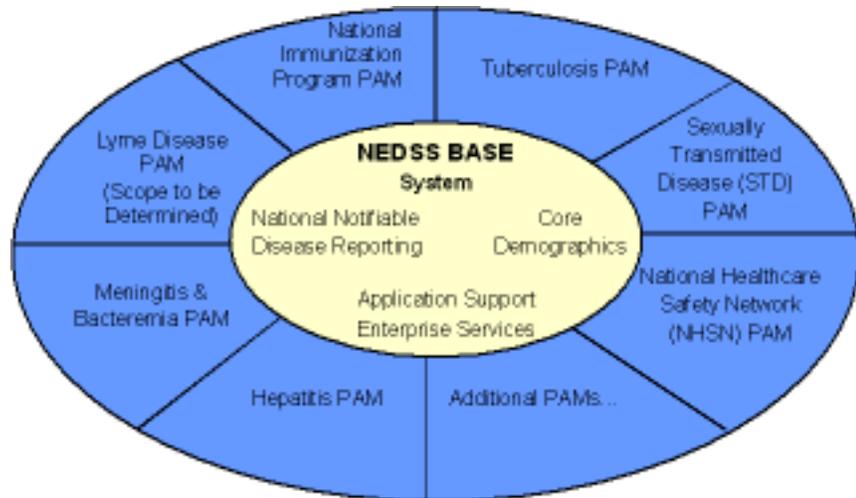


Figure 5. Conceptual design of NEDSS Base System.



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 orientation 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

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

Administrative

Identified Barrier. Facsimile transmission of PHI. (Transmission of PHI) (Scenario Three Patient Care C)

Proposed Solution: For stakeholders to adopt an interoperable means of PHI that does not rely on facsimile transmission as standard business practice and/or administrative procedure, technological advancements and solutions must first be in place.

General Context: Facsimile transmission was found to be the most common means of PHI transference (specifically in the case of nursing homes) although U.S. mail and courier methods were identified in some cases. The reason for this administrative policy was seen to be mistrust in alternate means, specifically doubts regarding the secure transmission of PHI via email.

Extent to which solution is in use: Members of UHIN utilize a secure method of electronic exchange with regards to administrative data. This is accomplished through an agreement among stakeholders with regards to policy regarding security and standards.

Identified Barrier. Transmission Security of PHI. [Scenario Three Patient Care C].

Proposed Solution: The use of current UHIN technology that could be further advanced to

accommodate for the transaction of clinical data. The demonstrated security could impact an entities decision to rely on PHI transmission in a secure manner that did not include fax.

General Context: The majority of stakeholders report transmitting PHI using a cover sheet that displays their identifying letterhead. The majority of substance abuse clinics responding indicate that they would also notify the receiving entity, by telephone, a fax was being transmitted and then would follow-up with a phone call to confirm. Although stakeholders believe that the current method is the most secure means available, it was confirmed by the SWG that the fabrication of hospital letterhead is indeed plausible and few, if any, would go to great lengths to confirm or verify the existence of requesting entity as the medical community relies heavily on an unspoken amount of trust.

Extent to which solution is in use: UHIN members are currently practicing the secure Internet transfer of administrative data.

Identified Barrier. Transmission security of PHI. [Scenario Three Patient Care C].

Proposed Solution: While the SWG did view that reluctance to allow access to PHI without a business agreement as a barrier to the interoperable exchange of information, the also view it as an effective practice to protect the privacy and the security of the healthcare consumer. As a result, it is determined that business practices and policies require a business agreement should remain in place even when such a transaction was allowed for under HIPAA treatment, payment, and healthcare operations.

General context: The majority of stakeholders report transmitting PHI using a cover sheet that displays their identifying letterhead. The majority of substance abuse clinics responding indicate that they would also notify the receiving entity, by telephone, a fax was being transmitted and then would follow-up with a phone call to

confirm. Although stakeholders believe that the current method was the most secure means available, it was confirmed by the SWG that the fabrication of hospital letterhead was indeed plausible and few, if any, would go to great lengths to confirm or verify the existence of requesting entity as the medical community relies heavily on an unspoken amount of trust.

Extent to which solution is in use: UHIN members are currently practicing the secure Internet transfer of administrative data.

Identified Barrier: Confusion regarding appropriate information sharing with first responders. (Authorization to Disclose) (Scenario Thirteen Bioterrorism)

Proposed 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.

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 Active Reporting System (POLARIS) serve as Utah's first responder data system (See Figure 4).

Identified Barrier: Reluctance to allow intra-agency access to PHI.
[Allowing Access to PHI - Scenario Fifteen Public Health A]

Proposed 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 5).

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 and, as a result, data cannot be easily exchanged, linked, or merged by personnel from different programs. Program managers also conveyed that they saw their program data as a resource and that they were responsible for maintaining a high level of control for the long-term benefit of their clients and the program itself. Program managers also express multiple concerns about data sharing that include misleading or misinterpretation of data, trust, and organizational transparency

Extent to which solution is in use: Policies are in place for limited sharing only. A system similar to Figure 4 was in the planning stages pending government funding approval. Separate data sets would remain independent while a central reporting database would communicate with all data sets and flag instances where health information overlaps. This eliminates the need for multiple systems that have little or no communication capability and improve the delivery of services to program recipients.

Legislative:

Identified Barrier: PHI governed by HIPAA and CFR 42 Part 2.

[Scenario Two Patient Care B].

Proposed Solution: Recommend federal legislation that maintains all PHI be protected equally.

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).

Extent to which solution is in use: Not applicable.

Educational

Identified Barrier. Lack of consumer understanding with regards to PHI privacy and security laws.

[Privacy and Security of PHI: Scenario Eight Law Enforcement].

Proposed Solution: Increase consumer awareness regarding their rights and responsibilities.

General Context: The majority of consumers remain uninformed as to what their rights were regarding the privacy and security of PHI. Many consumers and consumer groups fail to understand the concept of treatment, payment, or healthcare operations as allowed for under HIPAA and believe that their PHI was not release or viewe without their consent.

Extent to which solution is in use: Although web pages exist that explain HIPAA and the privacy and security rule, individuals are rarely concerned with viewing them until they feel that their rights have been infringed upon. Consumers are well aware that they sign a privacy and security document while seeing their provider but seldom ask questions or

bother to read the documents they sign.

Identified Barrier. Lack of education and/ or understanding of risks and realities of communicable diseases. [Providing education regarding risks and realities of communicable diseases - Scenario Fifteen Public Health A]

Proposed 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: A chasm exists between law enforcement first-responder personnel and medical personnel with regards to the dangers (both perceived and warranted) of communicable disease for first responders. 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.

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.

Identified Barrier. Lack of consumer understanding regarding the benefits to interoperable capability for health information exchange. [General :All relavent scenarios]

Proposed 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.

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 and 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.

6.2 Solutions to State Privacy and Security Laws/Regulations

Legal Workgroup proceedings determined that, with the exception of genetic testing, no business practices were driven by state legal drivers. Rather, tort or common law influenced the individual stakeholder business practices as advised by most legal counsel to provide extra protection above and beyond what was allowed for by HIPAA.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal statute governing various aspects of health information. In adopting HIPAA, Congress expressly intended to preempt contrary state law, unless state law is more stringent or a specific exception applies. [See 42 U.S.C. § 1320d-7]

Collaborative workgroups comprised of private and public representatives have come together to develop reference guides to assist public and private healthcare professionals and law enforcement to navigate situations where the right to access health information was in question. The workgroup applied standard preemption analysis to selected state laws that relate to the use or disclosure of health information. The analysis briefly describes the law or rule analyzed, indicates whether or not the Utah law or rule is consistent with HIPAA, cites the

specific section[s] of Title 45 of the Code of Federal Regulations, and provides a brief synopsis of the preemption analysis and in some instances additional code citations.

Access to private health information using a proper authorization is the easiest and fastest way to obtain documents. The workgroup developed a standard authorization form and outline of relevant laws to assist law enforcement officials to expeditiously access private health care information from health care entities in Utah.

6.3 Conflicting Federal and State Laws/Regulations

Contradictory legislation between the state and federal government did not exist with regards to the state of Utah.

6.4 Interstate e-Health Information Exchanges

The subject of Interstate e-Health Exchanges was not addressed by the SWG as most SWG members were present at the regional meeting and found similar business practices taking place. It was further determined that interoperability was to be more of a long-term solution between established RHIOs.

7.0 National-level Recommendations

Issues arose during the discussion of Scenario Two Patient Care B with regards to CFR 42 Part 2 and HIPAA. It was determined by the SWG that CFR 42 Part 2 was established prior to an era of electronic records and the need for interoperability and, while valiant in its efforts to add protection to substance abuse data, the regulation is perceived to be dated. It was further agreed upon that there was no consensus regarding what class of information requires "extra" protection.

SWG members agreed that all PHI should be afforded a high standard of protection, privacy, and security regardless of its class.

Appendix A.

RTI Standard Scenarios

Appendix A. RTI Standard Scenarios

Patient Care Scenario A

(The emergent transfer of health information between two healthcare providers when the status of the patient is unsure.)

Stakeholder entities:

- Hospital emergency room (requesting health information)

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89 year old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. There are questions concerning her possible impairment due to medications. Her adult daughter informed the ER staff that her mother has recently undergone treatment at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines there is a need to obtain information about Patient X's prior diagnosis and treatment during the previous inpatient stay.

Patient Care Scenario B

(The non-emergent transfer of records from a specialty substance treatment provider to a primary care facility for a referral.)

Stakeholder entities:

- Specialty substance abuse treatment facility (sending sensitive clinical records)
- Doctor's office or public health agency (receiving clinical records from the substance abuse facility)
- Client/patient

An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The two organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol relevant for medical diagnosis. The requested substance abuse information is being sent to the primary care provider. The primary care provider intends to refer the patient to a specialist and send all of his/her information including the substance abuse information received from the substance abuse treatment facility to the specialist.

Patient Care Scenario C

Stakeholders entities:

- Skilled Nursing Facility
- Physician
- Hospital

5:30pm Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psych unit to the nursing home. The hospital and skilled nursing facility are separate entities and do not share electronic record systems. At the time of the patient's transfer, the discharge summary and other pertinent records and forms were electronically transmitted to the skilled nursing home.

Upon entering the facility Dr. X seeks assistance in locating his patient, gaining entrance to the locked psych unit and accessing her electronic health record to review her discharge summary, I&O, MAR and

progress notes. Dr. X was able to enter the unit by showing a picture identification badge, but was not able to access the EHR. As it is Dr. X's first visit, he has no login or password to use their system.

Dr. X completes his visit and prepares to complete his documentation for the nursing home. Unable to access the skilled nursing facility EHR, Dr. X dictates his initial assessment via telephone to his outsourced, offshore transcription service. The assessment is transcribed and posted to a secure web portal.

The next morning, from his home computer, Dr. X checks his email and receives notification that the assessment is available. Dr. X logs into his office web portal, reviews the assessment, and applies his electronic signature.

Later that day, Dr. X's Office Manager downloads this assessment from the web portal, saves the document in the patient's record in his office and forwards the now encrypted document to the long-term care facility via email.

The skilled nursing facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

Patient Care - Scenario D

(The non-emergent transfer of health information.)

Stakeholder entities:

- Hospital mammography department (requesting health information)
- Outpatient Clinic (receiving request)

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the BrCa gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

Payment Scenario

(Note: This scenario is applicable to all healthcare providers.)

Stakeholder entities:

- Healthcare Provider (Hospital or Clinic)
- Health Plan (Payer)
- Patients

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the healthcare provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (e.g., emergency department records, clinic notes, etc.).

The health care provider has recently implemented an electronic health record (EHR) system. All patient information is now maintained in the EHR and is accessible to users who have been granted access

through an approval process. Access to the EHR has been restricted to the healthcare provider's workforce members and medical staff members and their office staff.

X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

RHIO Scenario

(Note: Each stakeholder should participate in this scenario keeping in mind the type of data their organization anticipates exchanging with a RHIO.)

Stakeholders entities:

- Multiple provider organizations
- Multiple RHIO's

The RHIO in your region wants to access patient identifiable data from all participating organizations (and their patients) to monitor the incidence and management of diabetic patients. The RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients.

Research Data Use Scenario

Stakeholder entities:

- Health care consumer
- Research investigator
- Health care provider
- Institution Review Board

A research project on children younger than age 13 is being conducted in a double blind study for a new drug for ADD/ADHD. The research is being sponsored by a major drug manufacturer conducting a double blind study approved by the medical center's IRB where the research investigators are located. The data being collected is all electronic and all responses from the subjects are completed electronically on the same centralized and shared data base file.

The principle investigator was asked by one of the investigators if they could use the raw data to extend the tracking of the patients over an additional six months and/or use the raw data collected for a white paper that is not part of the research protocols final document for his post doctoral fellow program.

Scenario for access by law enforcement

Stakeholder entities:

- Healthcare provider (providing health information)
- Law enforcement
- Patient
- Patient's family

An injured nineteen (19) year old college student is brought to the ER following an automobile accident. It is standard to run blood alcohol and drug screens. The police officer investigating the accident arrives in

the ER claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood alcohol test results and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff.

The patient is covered under their parent's health and auto insurance policy.

Pharmacy Benefit Scenario A

Stakeholder entities:

- Pharmacy Benefit Manager (requesting information)
- Outpatient Clinic (receiving request)
- Patient X

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy for a hospital which is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's Outpatient Clinic.

Pharmacy Benefit Scenario B

Stakeholder entities:

- Pharmacy Benefit Manager (requesting information)
- Company A
- Employees

A Pharmacy Benefit Manager 1 (PBM1) has an agreement with Company A to review the companies' employees' prescription drug use and the associated costs of the drugs prescribed. The objective would be to see if the PBM1 could save the company money on their prescription drug benefit. Company A is self insured and as part of their current benefits package, they have the prescription drug claims submitted through their current PBM (PBM2). PBM1 has requested that Company A send their electronic claims to them to complete the review.

Healthcare Operations and Marketing – Scenario A

[Note: This scenario could be modified to apply to any healthcare provider (physician group, home health care agency, etc.) wishing to market services to a targeted subset of patients.]

Stakeholder entities:

- Integrated delivery system (requesting study)
- Critical access hospital (being asked to provide health information)
- Tertiary hospital (being asked to provide health information)

ABC Health Care is an integrated health delivery system comprised of ten critical access hospitals and

one large tertiary hospital, DEF Medical Center, which has served as the system's primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports containing patient identifiable data to the system six-sigma team to analyze patient encounters and trends for the following rehab diagnoses/ procedures:

- Cerebrovascular Accident (CVA)
- Hip Fracture
- Total Joint Replacement

Additionally, ABC Health Care is requesting that this same information, along with individual patient demographic information, be provided to the system Marketing Department. The Marketing Department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

Healthcare Operations and Marketing - Scenario B

Stakeholder entities:

- Healthcare provider (Hospital obstetrics department)
- Hospital marketing department
- Patients

ABC hospital has approximately 3,600 births/year. The hospital Marketing Department is requesting identifiable data on all deliveries including mother's demographic information and birth outcome (to ensure that contact is made only with those deliveries resulting in health live births).

The Marketing Department has explained that they will use the PHI for the following purposes:

1. To provide information on the hospital's new pediatric wing/services.
2. To solicit registration for the hospital's parenting classes.
3. To request donations for construction of the proposed neonatal intensive care unit

They will sell the data to a local diaper company to use in marketing diaper services directly to parents.

Bioterrorism event

Stakeholder entities:

- Healthcare provider
- Public health department
- Law enforcement
- Government agencies
- Patients

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on

this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore this could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the State declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well informing the regional media to alert the public to symptoms and seek treatment if feel affected. The State also notifies the Federal Government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as they arise to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection

Employee Health Information Scenario

Stakeholder entities:

- Hospital emergency room (releasing health information)
- Employer human resources department (requesting health information)
- Employee

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has exacerbated which is not work-related. The employee's condition necessitates a four-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than 2 days leave. The hospital Emergency Department has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information via email to the Human Resources department of the patient's employer.

Public Health - Scenario A

(Active carrier, communicable disease notification.)

Stakeholder entities:

- Healthcare provider (primary care physician)
- Public health department
- Law enforcement
- Patient

A patient with active TB, still under treatment, has decided to move to a desert community that focuses on spiritual healing, without informing his physician. The TB is classified MDR (multi-drug resistant). The patient purchases a bus ticket - the bus ride will take a total of nine hours with two rest stops across several states. State A is made aware of the patient's intent two hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

Public Health – Scenario B

(Newborn screening)

Stakeholder entities:

- Healthcare provider (physician)

- State laboratory
- State public health department

A newborn's screening test comes up positive for a state-mandated screening test and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response system. The state lab also enters the information in its registry, and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

Public Health Scenario C

(Homeless shelters)

Stakeholder entities:

- Health care consumer
- Primary provider
- Drug treatment center
- Homeless shelter
- Patient relative

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. The person does have a primary provider, and is sent there for the medical care, and is referred to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement, and back to the shelter to verify that the person is in treatment. Someone claiming to be a relation of the homeless man requests information from the homeless shelter on all the health services the man has received. The staff at the homeless shelter is working to connect the homeless man with his relative.

Health Oversight: Legal compliance/government accountability

Stakeholder entities:

- State university faculty (requesting health information)
- State public health agencies (asked to provide health information)

The Governor's office has expressed concern about compliance with immunization and lead screening requirements among low income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient level health care data on an ongoing basis to determine if the children are getting the healthcare they need. This is not part of a legislative mandate. The Governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the Governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is not existing contract with the state university for services of this nature.

Appendix B.

Participating Stakeholders

Appendix B. Stakeholders Responding to Scenarios

STAKEHOLDER GROUPS	Number and Description of Participants
Clinicians	5 – a psychiatrist, a chiropractic clinician, a licensed RN research investigator, a practicing obstetrician who serves on administrative panels locally and nationally, and a licensed PA.
Physician groups	7 – A licensed pediatrician researcher, an obstetrician, a general practitioner, an ER physician, a family practitioner, a pediatrician, and an IT director .
Consumer/ Consumer Organization	16 – A single working mom, a representative from the state RHIO, a father of 4 children, a local undergraduate student and parents, an agent/broker for several self-insured employers, an employee of workman’s compensation fund of Utah, a physical therapist that specializes in elderly home care, a marketing employee for a pharmaceutical corporation, a patient advisor for a cancer education network, a department of health employee, a director of development at a local self insured company, an executive director of a clinic, an employee of the department of health, and an employee of a SA treatment center.
Hospitals	16 – A privacy and quality improvement officer, an ER physician at a tertiary hospital, radiological staff, file clerks, breast care coordinators at several tertiary hospitals, a manager of a HIPAA office at an IDS, an ER physician, a privacy officer at a hospital, a director of public relations/marketing for an orthopedic branch of an IDS, a professor and chair, a privacy officer at an IDS, two directors of nursing at separate medical centers, and an employee of the marketing department at a tertiary hospital.
Payers	3 – A regional healthcare IT specialist for a not-for-profit company, a privacy officer for the state retirement system, a representative from state Medicaid.
Public Health agencies	2 - A director and a practicing physician’s assistant at a public health agency.
Community clinics and health centers	5 - Director of a private, nonprofit program, an executive director at a state-licensed SA treatment center, a physician, a medical director whose clinic is part of an integrated deliver system, an office manager at a residential eating disorder facility.
Laboratories	2 – A medical director for a university owned laboratory, a respondent from the state laboratory.
Pharmacies	4 – One urban independent, one managed care, and one urban grocery store pharmacist, and an atypical pharmacist (chemo, in home, iv).
Long term care facilities and nursing homes	3 - The chief executive officer at a not-for-profit senior care facility, the financial service consultant for rehabilitation and extended nursing care facility, the director of nursing at a long term care facility.
State government (Medicaid, public health) depart-	6 – A representative from the office of epidemiology, a representative from the state Bioterrorism office, and the manager of data integration, an immunization program manager.
Law Enforcement	3 – An officer and chief of police in a mid-sized town, a representative from the FBI.
Medical and Public health research schools	3 – Director of IRB at local university, a senior compliance consultant of an IDS, and a pediatrician and assistant professor of pediatrics.
Other	2 – A fire fighter who responds in a Bioterrorism event and an HR director from a small to mid sized company.

RTI Form: Participating Stakeholders	HISPC WORK GROUPS					OUTREACH TO STAKEHOLDERS		
	Steering Committee	Variations Work Group	Legal Work Group	Solutions Work Group	Implementation Planning Work Group	Stakeholders providing input to variations assessment	Stakeholders providing input to solutions development and evaluation	Stakeholders providing input to implementation planning
Stakeholder Group	(X)	(X)	(X)	(X)	(X)	(N)	(X)	(X)
Clinicians	X	X		X	X		X	
Physicians and Physicians Groups	X	X		X	X	14	X	X
Federal Health Facilities	X							
Emergency Medicine		X	X	X	X	2	X	X
Hospitals / Health Systems	X	X	X	X	X	16		X
Community Clinics and Health Centers	X	X	X	X		3		
Mental Health and Behavioral Health	X	X	X	X		3		
Long Term Care Facilities and Nursing Homes		X				3		
Homecare and Hospice		X	X			3		
Laboratories						2		
Pharmacies / Pharmacy Benefit Managers	X	X				4		
Safety Net Providers								
Professional Associations and Societies	X	X						
Quality Improvement Organizations	X	X				1		
Medical and Public Health Schools / Research	X					3		
Public Health Agencies /Departments	X		X	X	X	4	X	X
Medicaid / Other State Government County Government	X			X		1		
Regional Health Information Organizations		X		X	X	1	X	X
Payers	X			X		3	X	
Individual Consumers		X				13		
Consumer Organizations and Advocates						1		
Employers						1		
Law Enforcement and Correctional Facilities		X		X		7		
Legal Counsel / Attorneys	X		X	X	X	4	X	X
Health Information Management organizations	X	X	X	X				
Privacy and Security experts / Compliance officers		X		X		3		
Health IT consultants	X						1	
Electronic Health Records experts		X		X	X			
Technology Organizations / Vendors								
Other (specify): _____								
Other (specify): _____								
Other (specify): _____								
Other (specify): _____								
Other (specify): _____								
Other (specify): _____								

Appendix C.

Utah Business Practice Data

Appendix C. Utah Business Practice Data

Patient Care - Scenario A

UT_01_01BP_patient_status

ER physician examines patient and obtains patient history. The ER Physician would also obtain information from officer on the scene.

Domain Information authorization and access controls

Stakeholder Hospitals

Legal Driver Emergency Medical Treatment and Active Labor Act requires that.

UT_01_02BP_information_to_treat

ER physician and nurse gather information directly from patient, if alert and oriented, or from family (adult daughter) if patient is not alert. The ER staff would also check for previous visits in our facility. This is done electronically or in rural settings by chart pull. ER physician requests medical information from neighboring state if needed.

Domain Information authorization and access controls

Stakeholder Hospitals

UT_01_03BP_requesting_patient_information

ER physician calls hospital in neighboring state to request a copy of the needed information during the day; would contact the medical records. After hours would contact ED or house supervisor. Mental health information would be requested on the phone call if the information were needed to treat the patient condition. Follow-up is done by fax.

Domain Information transmission security or exchange protocols

Stakeholder Hospitals

Legal Driver § 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. (c) Implementation specifications: Treatment, payment, or health care operations. (2) A covered entity may disclose protected health information for treatment activities of a health care provider.

§ 164.312 Technical safeguards. (d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.(h)(1) Standard: Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:(i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and (ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.(2) Implementation specifications: Verification.

UT_01_04BP_hospital_authentication

As an emergency room physician receiving a request from a physician in a neighboring state. I would get the following information - the hospital data (name of facility, fax number, physician name) over the phone. I would then verify the existence of the facility and physician on the Internet or our hospital database.

Domain	User and entity authentication
Stakeholder	Hospitals
Legal Driver	<p>§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. (c) Implementation specifications: Treatment, payment, or health care operations. (2) A covered entity may disclose protected health information for treatment activities of a health care provider.</p> <p>§ 164.514 Other requirements relating to uses and disclosures of protected health information.(h)(1) Standard: Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must: (i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and (ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart. (2) Implementation specifications: Verification.</p> <p>§ 164.312 Technical safeguards. (d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</p>

UT_01_05BP_transmit_medical_information

The emergency department would fax requested medical information to the requesting emergency room physician. If not an emergent situation, we would obtain a signed release by fax, either from patient if able, or next of kin. We would keep copy of releases, if applicable, and any faxes in medical record.

Domain	Information transmission security or exchange protocols
Stakeholder	Hospitals
Legal Driver	<p>§ 164.312 Technical safeguards.(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</p> <p>§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. (c) Implementation specifications: Treatment, payment, or health care operations. (2) A covered entity may disclose protected health information for treatment activities of a health care provider.</p> <p>§ 164.514 Other requirements relating to uses and disclosures of protected health information.(h)(1) Standard: Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:(i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and (ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.(2) Implementation specifications: Verification.</p>

UT_01_06BP_receiving_request_for_patient_information

As an emergency room physician receiving a request for patient information I have the requesting physician provide patient's name, date of birth & date of service on their letterhead sent to us by fax. I ask for their telephone number, and then call them back to verify their location.

Domain	User and entity authentication
Stakeholder	Hospitals
Legal Driver	<p>§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. (c) Implementation specifications: Treatment, payment, or health care operations.(2) A covered entity may disclose protected health information for treatment activities of a health care provider.</p> <p>§ 164.514 Other requirements relating to uses and disclosures of protected health information. (h)(1) Standard: Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:(i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and (ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.(2) Implementation specifications: Verification.</p> <p>§ 164.312 Technical safeguards.(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</p>

Patient Care - Scenario B

UT_02_01-1BP_patient_authorization_to_release_PCP_to_SPEC

We have "release of information" forms readily available. The form must be specific to the information being exchanged and the agencies exchanging the information. The primary care provider has a conversation with the client explaining what the form means and then requests a signature.

Domain	Information authorization and access controls
Stakeholder	Public health agencies
Legal Driver	42 CFR §2.32 Prohibition on redisclosure. Notice to accompany disclosure. Each disclosure made with the patient's written consent must be accompanied by the following written statement: This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

UT_02_01-2BP_patient_authorization_to_release_PCP_to_SPEC

I refer patients to the specialist and the specialist determines what information is needed from my patient record. The specialist initiates the authorization on their end by getting the patient's signature authorizing me to release their patient information.

Domain	Information authorization and access controls
Stakeholder	Community clinics and health centers
Legal Driver	42 CFR Part 2 §2.12 a federally assisted substance abuse treatment program is restricted from disclosing information that would identify a patient in a substance abuse treatment program without the patient consent. Consent must be obtained even to forward records to another treating provider that is outside the substance facility. 42 CFR §2.12. No consent is required if the disclosure is made to treating personnel in a medical emergency situation because of a crime on the premises, audit, program evaluation, or pursuant to court order §2.51, 2.52, 2.61. Providers are prohibited from re-disclosing information from a substance abuse treatment program. § 2.3 Thus patient consent is required by 42 CFR Part 2 to release information from

the substance abuse treatment program to the primary care provider, and consent would be required again to sent the information on to the specialist.

UT_02_01BP_patient_authorization

When a substance abuse facility refers a patient to a primary care provider, a clinician, case manager, or counselor asks the patient to sign a 42-C.F.R. compliant release of information which specifies the type of information to be shared, the name of the primary care provider, length of time the release is valid, etc. On our releases it is stipulated that confidential information not be passed on to parties outside of the scope of the release.

Domain Information authorization and access controls

Stakeholder Community clinics and health centers

Legal Driver 42 CFR Part 2 §2.12 a federally assisted substance abuse treatment program is restricted from disclosing information that would identify a patient in a substance abuse treatment program without the patient consent. Consent must be obtained even to forward records to another treating provider that is outside the substance facility. 42 CFR § 2.12. No consent is required if the disclosure is made to treating personnel in a medical emergency situation because of a crime on the premises, audit, program evaluation, or pursuant to court order §2.51, 2.52, 2.61. Providers are prohibited from re-disclosing information from a substance abuse treatment program. § 2.3 Thus patient consent is required by 42 CFR Part 2 to release information from the substance abuse treatment program to the primary care provider, and consent would be required again to sent the information on to the specialist.

UT_02_02BP_determining_information_to_be_sent

Once the substance abuse facility has the patient sign an authorization, not all information needs to go. We will only send the minimum necessary that should be sent (treatment plan, medication review). Moreover, we will only send SA information if it has to do with the suspected medical problem.

Domain Information authorization and access controls

Stakeholder Community clinics and health centers

UT_02_03BP_facility_authenticating

After receiving a request for information from a primary care provider we, a substance abuse clinic, would call the provider, especially if they were not known to us. In some cases, we ask them to mail or fax a written request on letterhead.

Domain User and entity authentication

Stakeholder Community clinics and health centers

Legal Driver § 164.312 Technical safeguards.(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

UT_02_04BP_transmission_non-electronic_SA_to_PCP

Once the release form is signed at the treatment center, the case manager/counselor would copy the necessary records and forward them generally by mail, courier, or have a member from the primary care providers office pick them up. They will be in a sealed envelope, and the person who receives the records will need to sign a receipt.

Domain Information transmission security or exchange protocols

Stakeholder Community clinics and health centers

Legal Driver § 164.530 Administrative requirements.(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

UT_02_05-1BP_transmission_PCP_to_SPEC

As primary care provider I get the information to the specialist so treatment can continue.

Generally, I call the specialist to discuss patient history and then fax the medical record to their office. Sometimes it would be mailed.

Domain Information transmission security or exchange protocols
 Stakeholder Public health agencies
 Legal Driver 42 CFR §2.32 Prohibition on redisclosure. Notice to accompany disclosure. Each disclosure made with the patient's written consent must be accompanied by the following written statement: This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

UT_02_05BP_transmission_electronic_SA_to_PCP

We would obtain a signed "consent to release" information form from patient before sending any information to the specialist. The substance abuse counselor calls the primary care office to verify the number and alert their staff that we will be sending a release form to them. We ask that authorized receiver be near the fax when the data is sent. We receive a faxed response to verify that the information was received. We use a fax cover sheet stamped "re-disclosed prohibited". The cover sheet is also printed with the full CFR 42 Part II disclosure prohibition. At present we only transmit by fax, as it is our understanding that email is not acceptable externally.

Domain Information transmission security or exchange protocols
 Stakeholder Public health agencies
 Legal Driver § 164.530 Administrative requirements.(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

42 CFR §2.32 Prohibition on redisclosure. Notice to accompany disclosure. Each disclosure made with the patient's written consent must be accompanied by the following written statement: This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

UT_02_06BP_verifying_receipt_of_record

When our treatment facility sends medical information we get a signed receipt from the requester on any and all records received. If they go by mail, by courier, hand delivered or picked up, they need to be signed for. Receipt is kept in the patient chart.

Domain User and entity authentication
 Stakeholder Community clinics and health centers

UT_02_07BP_logging_disclosures

After the substance abuse facility sends patient information to the primary care physician the counselor logs the information on a form in the client's file at the substance abuse facility, even in the case where the patient has authorized the release.

Domain Information use and disclosure policy
 Stakeholder Community clinics and health centers

UT_02_08BP_recording_access_to_SA_PHI

The treatment facility keeps the original authorization form in patients charts. Any person

copying these records must put their name and date that the copies were made on the authorization form. We also record the date mailed to primary care provider, or sent/picked up date. Once receipt of delivery is received by us, then we put it with the authorization, and they are kept together at all times.

Domain Information use and disclosure policy
Stakeholder Community clinics and health centers

UT_02_09-1BP_storage_of_SA_PHI_restricted_access

When we do receive patient information from a treatment facility it is kept in the patient's chart with access to the chart restricted to those employees and volunteers who have been given direct access. All volunteers and paid employees sign a confidentiality form. Our clinic considers SA information to be highly confidential.

Domain Administrative or physical security safeguards
Stakeholder Public health agencies
Legal Driver § 164.514 Other requirements relating to uses and disclosures of protected health

information.(d)(1) Standard: Minimum necessary requirements. In order to comply with §164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.(2) Implementation specifications: Minimum necessary uses of protected health information.(i) A covered entity must identify:(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

UT_02_09BP_storage_of_SA_PHI

Our substance abuse facility keeps PHI in individual client records, which are double locked (in a locked cabinet behind locked door). Other information, such as immunization records, medication logs, etc., are stored in medical file in the nurse's office.

Domain Administrative or physical security safeguards
Stakeholder Community clinics and health centers
Legal Driver 42 CFR §2.16 Security for written records.(a) Written records which are subject to these

regulations must be maintained in a secure room, locked file cabinet, safe or other similar container when not in use; and(b) Each program shall adopt in writing procedures which regulate and control access to and use of written records which are subject to these regulations.

UT_02_10BP_patient_consent_to_treat_PCP

As the primary care physician receiving the referral from the substance abuse treatment facility I would obtain a "consent to treat" form from the substance abuse client before seeing the patient.

Domain Information authorization and access controls
Stakeholder Public health agencies

UT_02_CS1

The primary care provider, nurse assistants, etc., will have access, which is acceptable given appropriate client consent. The primary care provider should not re-release this information without consent from the client.

Domain Information authorization and access controls
Stakeholder Consumers or consumer organizations

UT_02_CS2

Most clients feel this is acceptable and necessary. For those trying to stay clean, they want their provider to be sensitive regarding what sorts of medication he/she prescribes so their sobriety is not compromised.

Domain Information use and disclosure policy
Stakeholder Consumers or consumer organizations

Patient Care - Scenario C

UT_03_01-1BP_business_agreements_LTC

Our long term care facility has business associate agreements. However, a medical provider does not need to have such an agreement as long as he/she is involved in the provision of treatment or the plan of care.

Domain Information authorization and access controls
Stakeholder Long term care facilities and nursing homes

UT_03_01BP_business_agreements_physician

Our physician office has business associate agreements in place that provide for the sharing of data among treatment providers involved in the direct care of patients.

Domain Information authorization and access controls
Stakeholder Clinicians

UT_03_02BP_security_training_LTC

All staff (and volunteers) in our psych unit receive training in data security and are required to sign a privacy agreement. Access to electronic records would be a problem, we do not share passwords or have available sharable passwords.

Domain Administrative or physical security safeguards
Stakeholder Clinicians
Legal Driver

§ 164.310 Physical safeguards. A covered entity must, in accordance with §164.306: (a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

UT_03_03BP_access_mental_health-info

In our long term care facility we would give a treatment provider access to their patient's record. Our facility grants access based on a need to know. Direct care employees on specific units are allowed access to that units patient information. Employees on other units would not have access to the psych unit. In the case of the psych unit, their staff would have a specific login and password to access that unit's information.

Domain Administrative or physical security safeguards
Stakeholder Long term care facilities and nursing homes
Legal Driver

§ 164.514 Other requirements relating to uses and disclosures of protected health information.(d)(1) Standard: Minimum necessary requirements. In order to comply with §164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.(2) Implementation specifications: Minimum necessary uses of protected health information.(i) A covered entity must identify:(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

UT_03_04-1BP_temporary_electronic_access_to_LTC_records

When a new admission is made to the long term care facility the patient's doctor would be given a log-in and password to the electronic medical records program through the IT dept. A copy of this information is placed in the patient's chart in case the doctor was to forget or lose that information.

Domain Information authorization and access controls
Stakeholder Long term care facilities and nursing homes

Legal Driver § 164.310 Physical safeguards. A covered entity must, in accordance with §164.306:(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

§ 164.530 Administrative requirements.(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

UT_03_04BP_temporary_access_to_LTC_records

A physician, psychiatric nurse, nurse practitioner etc. is required to be credentialed and privileged prior to the time that our long term care facility can accept orders. This includes allowing access to their patient's mental health record. If a patient or their surrogate, requests a non-credentialed physician or specialist we require documentation of license, education, and other basic information that can be utilized to obtain verification of the person's credentials. We usually obtain verification within 24 hrs. after receiving information.

Domain Information authorization and access controls
Stakeholder Long term care facilities and nursing homes

UT_03_05BP_receive_fax_transmission_patient_info

Our long term care facility asks outside entities to notify the intended recipient prior to faxing protected health information (PHI), in order to assure that the appropriate person removes it from the fax machine without disclosure to other people. Unfortunately, few of the outside entities are consistent about the advance call. There is little use of electronic transmission of patient information with the exception of fax.

Domain Information transmission security or exchange protocols
Stakeholder Long term care facilities and nursing homes

Legal Driver § 164.530 Administrative requirements.(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

§ 164.312 Technical safeguards.(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

UT_03_06BP_transmission_mental_health_data_electronic

In our psych unit we would fax the patient record and would not send it by encrypted email. The record would be faxed so that there would be a paper copy in the patient chart. The email document would be encrypted and the facility would need the key. Most likely the facility would not have the key and to alleviate any issues, we would simply fall back on faxing the documents.

Domain Information transmission security or exchange protocols
Stakeholder Clinicians

Legal Driver § 164.530 Administrative requirements.(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

UT_03_07BP_storage_of_mental_health_phi

All hard copy patient charts are under lock and key when not in direct use by staff in our long term care facility.

Domain Administrative or physical security safeguards
Stakeholder Long term care facilities and nursing homes

Legal Driver § 164.530 Administrative requirements.(c)(1) Standard: Safeguards. A covered entity must have

in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

Patient Care - Scenario D

UT_04_01BP_authorization_to_release_information

At our hospital the physician or nurse at our mammography clinic would request an appropriate release from the patient to allow for the request of her mammography films from another entity.

Domain Information authorization and access controls

Stakeholder Hospitals

UT_04_02BP_authenticate_entities

Our mammography clinic verifies any entities that request information or an entity from which a patient hand delivers films. We do this by calling the accreditation office - we also call the institution if there is a question. Most requests for patient information are physician to physician by phone when requesting records or patient information.

Domain User and entity authentication

Stakeholder Community clinics and health centers

Legal Driver § 164.312 Technical safeguards (d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

UT_04_03BP_need_to_know

As a physician in a hospital mammography department I would not need HIV information to perform a screening mammogram on this patient. HIV should only be released to those health care providers that "need to know". Our hospital follows HIP AA policy.

Domain Information authorization and access controls

Stakeholder Hospitals

Legal Driver § 164.514 Other requirements relating to uses and disclosures of protected health information (3) Implementation specification: Minimum necessary disclosures of protected health information (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

UT_04_04BP_release_of_deceased_medical_information

As the physician, the release of genetic information of a deceased patient requires a signed statement from the deceased relatives next of kin or executor of the deceased's estate authorizing the release of that information. Next of kin is the closest living relative.

Domain State law restrictions

Stakeholder Hospitals

Legal Driver Utah code 78-25-26 Access to medical records of deceased patient. For purposes of Section 78-25-25, and 45 C.F.R., Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information, a health care provider with medical records of a deceased person may recognize the deceased person's surviving spouse or an adult child as a personal representative.

UT_04_05BP_transmit_mammogram_digital

In our Integrated Delivery Systems' radiology departments, the radiology tech copies the images to a cd for the patient to take with them or the images are made available to the physician via the internet using the picture archive communication system (PACS). While we have this capability, it is rarely used as the preferred media is film and we print hard copy film for physicians and institutions. We rarely receive digital cd mammogram files from patients.

Domain Information transmission security or exchange protocols
Stakeholder Hospitals
Legal Driver § 164.312 Technical safeguards.(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

UT_04_06BP_transmit_mammogram_film

In our radiology department most mammograms are films. We require patient consent to release and a 24 hour notice to provide patient films for pick-up by the patient or a personal representative with a photo ID and patient authorization. The films are usually sent and received by mail or courier.

Domain Information transmission security or exchange protocols
Stakeholder Hospitals
Legal Driver § 164.508 Uses and disclosures for which an authorization is required (6) Documentation.(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

§ 164.530 Administrative requirements (c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

Payment Scenario

UT_05_01-1BP_authorization_to_release_patient_information

If a payer needs access to EMR to authorize in-patient encounters, we, the payer, would not necessarily need patient authorization under the assumption that the provider has had the patient sign a release of information form allowing the provider to send information to the payer.

Domain Information use and disclosure policy
Stakeholder Payers

UT_05_01BP_authorization_to_release_patient_information

In our clinic we make sure that all patients, before treatment, have submitted a release (authorization form) for access to occur.

Domain Information use and disclosure policy
Stakeholder Clinicians

UT_05_02BP_Access_control_to_patient_info

We, a patient clinic, would not grant direct access to a patient's health information record. If a payer wanted more information for billing purposes, they would have to tell us what information they required, the office manager would then code the patient's information from the record into a standard format for billing. Patient information is restricted to clinic staff only. The required information is then submitted to the payer through our RHIO.

Domain Information authorization and access controls
Stakeholder Clinicians

UT_05_03BP_sharing_patient_data_agreement

As a payer if we need access to a provider's Electronic Health Record (EHR) but the EHR has been restricted to the provider's work force members, office staff only, we would provide substantive evidence of administrative savings and a decrease in lapsed time for payment as incentive for the provider to want to provide access. Then partner with the hospital to establish the most appropriate way of managing security and privacy.

Domain Administrative or physical security safeguards
Stakeholder Payers

UT_05_04-1BP_minimum_necessary_required_for_transmission

Because clinics are covered entities, we, a payer, require record requests to contain at least the following information to be within HIPAA guidelines. clients name, ssn, DOB; specific health info; purpose of request; patient signature/date; expiration date; specific identification HCU (health care user number) is requested to disclose; specific identification of recipient of info; specific statement of patient’s rights; a covered entity may not condition failure to sign; potential for re-disclosure w/o privacy protections.

Domain Information authorization and access controls
Stakeholder Payers

UT_05_04BP_minimum_necessary_required_for transmission

As a payer, we have established minimum data needs based on category of service. With the larger providers we may agree on specific reports, such as discharge summaries, to serve as the minimum data needed for many of the inpatient claims.

Domain Information authorization and access controls
Stakeholder Payers

UT_05_05BP_transmission_of_data

The mechanism for us, the payer, for receiving the information from the provider is generally not specified in the patient release. Assuming that we have access to the EMR (electronic medical record) and this access is role based and either limited to specific necessary areas of the EMR or allowed logged specific views depending on the need, that is, specific reports or views could be developed within the EMR designed for payers.

Domain Information transmission security or exchange protocols
Stakeholder Payers

UT_05_CS3

If a clinic has an electronic health record database, then they would be able to put parameters in the system to be able to tell who, when, where, and why did a clinic staff member enter a patient record. Internal audit should be made to make sure clinic staff members are being ethical in every aspect of patient record confidentiality.

Domain Information audits and record and monitor activity
Stakeholder Consumers or consumer organizations

UT_05_CS4

Access should only be allowed for direct care clinic personnel. They would need to have a specific reason for entering/viewing the records of a patient. Access should only be allowed for billing related to that specific incident.

Domain Information authorization and access controls
Stakeholder Consumers or consumer organizations

UT_05_CS5

Any personal health information including name, ssn, etc., would not be sent to any person, or entity, without my clear consent on who it is being sent to, and the allowable information being sent.

Domain Information authorization and access controls
Stakeholder Consumers or consumer organizations

UT_05_CS6

If I, a consumer, wanted my information released to a payer, I would sign an authorization form at my health care provider’s office.

Domain Information use and disclosure policy
Stakeholder Consumers or consumer organizations

RHIO Scenario

UT_06_01BP_Exchange_phi_between_providers

The RHIO exchanges patient information between two Utah RHIO members. Exchanges of patient information for quality measurement purposes between members can be facilitated by the Utah RHIO, but the RHIO does not monitor, store, or analyze any of this data.

Domain Information transmission security or exchange protocols
Stakeholder Professional associations and societies

UT_06_02BP_PHI_RHIO_new_exchange_coordination

The RHIO is a member based organization. If a business need is identified regarding organizations that would like to exchange/submit patient information from one organization to another, a request is made to the Utah RHIO Standards Committee for chartering a subcommittee to develop a community standardized message.

Domain Information transmission security or exchange protocols
Stakeholder Professional associations and societies

Research Data Use Scenario

UT_07_01-1BP_IRB_approval_post-doc

As principal investigator I would have post-doc file his/her own IRB

Domain Information use and disclosure policy
Stakeholder Clinicians

UT_07_01-2BP_IRB_approval_by_IRB

As the IRB, we require the study to resubmit when there are procedural changes. This includes re-consent via a parental permission document and children aged 7 to 17 would receive an updated assent document. We would then review the contents of all proposed consents/authorizations for research to determine if they are compliant with both human subjects research regulations and the privacy rule.

Domain Information use and disclosure policy
Stakeholder Medical and public health schools that undertake research
Legal Driver

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required (2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the criteria.

§ 164.502 Uses and disclosures of protected health information: general rules.(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

§ 164.508 Uses and disclosures for which an authorization is required. (c) Implementation specifications: Core elements and requirements.(1) Core elements.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.(i) Standard: Uses and disclosures for research purposes.(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:A) An Institutional Review Board (IRB), orB) A privacy board Have met specified conditions.

UT_07_01BP_IRB_approval_PI

As the Principal Investigator, I would amend the study to include the new use of the raw data and an additional six months tracking for the white paper and submit the amendment to IRB for expedited process. This occurs whether or not the drug company is maintaining the centralized database.

Domain
Stakeholder
Legal Driver

Information use and disclosure policy

Clinicians

§ 164.502 Uses and disclosures of protected health information: general rules.(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.(i) Standard: Uses and disclosures for research purposes.(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that: (i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either: (A) An Institutional Review Board (IRB), or (B) A privacy board Have met specified conditions.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required (2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following: (ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

§ 164.508 Uses and disclosures for which an authorization is required. (c) Implementation specifications: Core elements and requirements.(1) Core elements.

UT_07_02BP_parental_consent_bypass_PI

As principal investigator, I would see if original consent form specified how long data would be collected. It might be that extending data collection for six months would simply mean checking with IRB to ensure compliance. For the use of data for a purpose it was not originally intended for, I would again check original consent form to see if it included a clause that allowed for the use of secondary analysis.

Domain
Stakeholder
Legal Driver

Information use and disclosure policy

Clinicians

§ 164.502 Uses and disclosures of protected health information: general rules.(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.(i) Standard: Uses and disclosures for research purposes.(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:A) An Institutional Review Board (IRB), or B) A privacy board Have met specified conditions.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.(2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of

authorization satisfies the criteria.

§ 164.508 Uses and disclosures for which an authorization is required. (c) Implementation specifications: Core elements and requirements.(1) Core elements. A valid authorization under this section must contain at least the elements.

UT_07_03BP_obtain_parental_re-consent_PI

As principal investigator I (or my post-doc researcher) would ask participants at one of their personal contact visits to sign a new consent form. If no face-to-face contact with the study participants occurs then a letter with an explanation, a phone number to call in case of questions, and a SASE to return the signed consent witnessed by a friend or family member would be forwarded. Subjects under 13 would require both parental consent and subject assent. The electronic file should include a verification that there is assigned IRB approval consent and authorization of file and what version it is and when it was signed. The re-consent would be posted to the database so it could be reviewed.

Domain Information use and disclosure policy

Stakeholder Clinicians

Legal Driver § 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.(2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the criteria.

UT_07_04BP_parental_consent_IRB_bypass

The IRB would encourage the principal investigator to submit the new project as a data-only project using existing research data. The investigator could then apply for a waiver of authorization as permitted in the privacy rule 45 CFR 164.512(l).

Domain Information use and disclosure policy

Stakeholder Medical and public health schools that undertake research

Legal Driver § 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.(i) Standard: Uses and disclosures for research purposes.(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:A) An Institutional Review Board (IRB), orB) A privacy board Have met specified conditions.

UT_07_CS7

If I agreed to have my child participate in a research study and the principle investigator was asked by one of the investigators if they could use the raw data to extend the tracking of my child for an additional 6 months and use that data for a white paper that was not part of the original research protocol, as a consumer (parent of 13 year old child), my concern would be that the findings (specifically my child's) from the study be used in a way that I was aware of upfront. I would not want my child's information used for other "white papers" or additional research that I did not consent to upfront. Consent for all uses of the data should be obtained up front. If additional uses are identified after the fact, I would expect the investigator to obtain consent from myself to use my child's information.

Domain Information use and disclosure policy

Stakeholder Consumers or consumer organizations

Scenario for access by law enforcement

UT_08_01BP_blood_alcohol_sample_law_enforcement

For law enforcement, if we suspect alcohol is involved we ask permission to obtain an alcohol level. Failure to comply can result in the loss of driving privilege. In cases where there is a risk of fatality we do not ask permission as we have a contract with county paramedics to do the draw at the accident site before transport to the hospital. Once the patient enters the hospital it becomes increasingly difficult to get information without a court order or subpoena.

Domain State law restrictions
Stakeholder Other Specified Law Enforcement

UT_08_02BP_patient_status

As an ER physician my first concern would be to treat the patient.

Domain Information authorization and access controls
Stakeholder Hospitals

UT_08_03BP_release_of_medical_information_hospital_to_law

Our hospital does not have a contract with law enforcement for blood draws but we do them if requested for our own health treatment purposes only. The results cannot be released without patient's authorization or a valid legal document. The hospital blood results are usually in different unit measures than the unit measures that law enforcement uses.

Domain Information use and disclosure policy
Stakeholder Hospitals

UT_08_04BP_release_of_medical_information_hospital_to_insurance

Our hospital cannot release medical information without the patient's authorization. However, if the insurance company is part of TPO (treatment, payment, and operations), and when they request medical records, we can release them. There is one caveat, if they contain any sensitive material (i.e. drug or alcohol related information) the patient must be contacted and permission given before the medical records can be released.

Domain Information use and disclosure policy
Stakeholder Hospitals
Legal Driver § 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required. A covered entity (such as the Hospital) is required to disclose the results of the blood test to the law enforcement official only if the law enforcement official provides a court order, a subpoena or summons ordered by a judge, an administrative subpoena or summons, authorized investigative demand, or similar process authorized under state law.

UT_08_05BP_release_of_medical_information_hospital_to_parent

Our hospital cannot release medical information to parents without the patient's authorization. However, if the insurance is on the parents policy, parents can ask for billing information (treatment, payment, and operations), and we can release them.

Domain Information use and disclosure policy
Stakeholder Hospitals
Legal Driver 45 CFR 164.506 allows for the disclosure for "TPO";

42 CFR Part does not apply - misunderstanding of 42 CFR Part 2. It does not apply because the patient is not in a substance abuse treatment program.

UT_08_06-1BP_obtaining_medical_information_from_hospital

For law enforcement to get a copy of an individual's medical information that was involved in an accident investigation, we would have to subpoena the records. We first would try to get the person's consent at the accident scene and get as much information as possible from the individual at the scene. The subpoena process involves serving the subpoena, often waiting two weeks for a reply. Then we either get a call to let us know the record is ready for pick up or that it was mailed. The investigator will, in most cases, go to the hospital to get the report.

Domain Information use and disclosure policy
Stakeholder Other Specified Law Enforcement

UT_08_06BP_obtaining_medical_information_from_hospital

As law enforcement, we can talk to anyone without authorization, but we have a very difficult time getting information from primary care doctors as they don't want to have to spend time testifying in court. In some situations the ER doc will talk "off the record" in a general sense about the accident and injuries sustained by the individual to compare consistency of injury with facts gathered to date. The ER docs will also give officers updates on the general status of the individual but in a very broad sense, (e.g. doing better or not going to make it). The specific detail or information that would be officially documented for the investigation would be obtained through a subpoena. We try to get relevant information collected before the individual gets to the hospital.

Domain Information use and disclosure policy
Stakeholder Other Specified Law Enforcement

UT_08_CS10

From patient perspective: No one can have my information unless I give them access to it. Sometimes we sign so many things I think I've given away my first three children and they are not even born yet. From parent's perspective: I would talk with the doctor and ask what the standard protocol is and then the police officers. I believe that the police can ask for the information and we can refuse. They would have to get a court order to get it, but then they could place him, the driver, under arrest. I would be inclined to let him face the consequences of his action though.

Domain Information use and disclosure policy
Stakeholder Consumers or consumer organizations

UT_08_CS8

I think the EMTs do it automatically as part of the blood work if it's for an accident and the cops show up. So I'd have to say they must have some kind of arrangement. But I know you can also say no to the police, I saw it on TV. You have to know that they can arrest you, but still you can always say no. But since I wasn't drinking I wouldn't care if they had the results, unless the lab got it wrong, I saw that on TV too.

Domain State law restrictions
Stakeholder Consumers or consumer organizations

UT_08_CS9

As a parent, for the doctor to ask the patient if it's OK to talk in front of his parents is weird. Unless he's not conscious or can't communicate, then I guess he'd just talk to us because we'd be the next of kin or responsible party - the checkbook.

Domain Information use and disclosure policy
Stakeholder Consumers or consumer organizations

Pharmacy Benefit - Scenario A

UT_09_01BP_authorization_to_disclose_patient_info_for_prescription_fill

As the health care provider, sharing information with the pharmacy may not be an issue because I only need to give them a new prescription for the new medication if the patient decided not to pay out of pocket. I don't need to give them diagnostic information necessarily or any personal info they do not already have. In my consent paperwork, that all clients fill out, I educate them about other agencies, including their insurance agency, that may need information about diagnosis and treatment plan information. I explain to them that all insurance agencies as part of the terms of coverage have a clause giving them access to that information if the client uses their insurance to pay for their visit and or medication.

Domain Information use and disclosure policy
Stakeholder Clinicians
Legal Driver Physician, pharmacy, and PBM may each use or disclose protected health information for their

own treatment, payment, or health care operations (“TPO”), because all are presumably covered entities under HIPAA. 45 CFR 164.506(c)(1). Physician, pharmacy, and PBM may each be viewed as a covered entity under HIPAA because each is a health care provider.

UT_09_02BP_PHI_sent_from_PCP_to_pharmacy

As a nurse practitioner, it is my understanding that the pharmacy only requires the medication, patient name and date of birth. They require my state license number and sometimes a DEA number. The insurance company may require a diagnostic code to cover medication. If they request more information I discuss it with the client first and get their approval before disclosing further information.

Domain Information use and disclosure policy

Stakeholder Clinicians

Legal Driver § 164.514 Other requirements relating to uses and disclosures of protected health information. The “minimum necessary” rule in 45 CFR 164.514(d) applies to the interactions between physician, pharmacy, and/or PBM. If one of the parties requests from the other information not relevant to treatment, patient, or health care operations, this would generally be prohibited by HIPAA both because the minimum necessary rule would have been violated and because the interaction would no longer fit within the definition of treatment, payment, or health care operations. The different parties involved must limit the types of persons who receive the patient information as well as the types of patient information received.

UT_09_03BP_PHI_sent_from_pharmacy_to_PCP

As a pharmacist the only information about the particular prescription is shared with the prescribing physician. Minimal information is disclosed in the process (name, date of birth, medication, insurance information).

Domain Information use and disclosure policy

Stakeholder Pharmacies

Legal Driver § 164.514 Other requirements relating to uses and disclosures of protected health information. The “minimum necessary” rule in 45 CFR 164.514(d) applies to the interactions between physician, pharmacy, and/or PBM. If one of the parties requests from the other information not relevant to treatment, patient, or health care operations, this would generally be prohibited by HIPAA both because the minimum necessary rule would have been violated and because the interaction would no longer fit within the definition of treatment, payment, or health care operations. The different parties involved must limit the types of persons who receive the patient information as well as the types of patient information received.

UT_09_04BP_Pharmacy_communication_with_patient_and_physician

As a pharmacy we would inform the patient that the medication is not on their formulary and not on the preferred alternative list, so we would ask them if they would like to pursue the prior authorization. If so, we would fax the prescribing physician only the information necessary to obtain the prior authorization.

Domain Patient and provider identification

Stakeholder Pharmacies

Legal Driver 45 CFR 164.506(c)(1) Physician, pharmacy, and PBM may each use or disclose protected health information for their own treatment, payment, or health care operations (“TPO”), because all are presumably covered entities under HIPAA. 45 CFR 164.506(c)(1). As health care providers and covered entities under HIPAA, physician, PBM, and pharmacy can freely interact with patient for TPO purposes, including obtaining additional information from patient, or giving additional information to patient. In addition, as covered entities, PBM, pharmacy, and physician can disclose patient information to each other and to other entities for treatment purposes. 45 CFR 164.506(c)(2). Thus, PBM, pharmacy, and physician can each talk to patient and to each other regarding filling the Geodon prescription without the need to obtain a patient authorization.

§ 164.514 Other requirements relating to uses and disclosures of protected health information. The “minimum necessary” rule in 45 CFR 164.514(d) applies to the interactions between

physician, pharmacy, and/or PBM.

UT_09_05BP_acknowledgment_receipt_HIPAA_policy

With our pharmacy, the patient receives a copy of the HIPAA rules and regulation along with our pharmacy's privacy practices and signs an acknowledgment of receipt.

Domain Information use and disclosure policy

Stakeholder Pharmacies

UT_09_06BP_PCP_communication_with_patient

I, the primary care provider, would verify with the patient that they submitted the prescription and talk with them about confidentiality. I would also explain that they can get the Geodon but will have to pay out of pocket or that they could use one of the alternatives. I would explain the similarities and differences between the choices and recommend the best alternative.

Domain Information use and disclosure policy

Stakeholder Clinicians

UT_09_CS11

Those individuals that have a need to know to get their job done or to provide care and services to patients. There is a risk in allowing everyone access to all information. Safeguards need to be in place to protect patients as well as those workers involved in providing services.

Domain Information authorization and access controls

Stakeholder Consumers or consumer organization

UT_09_CS12

The doctor should and the pharmacy should have access to patient information to fill the prescription. It is a current fill and it is generated by the patient. The medication not being on the formulary should not require a new signature for authorization. It's the same prescription trying to be filled.

Domain Information authorization and access controls

Stakeholder Consumers or consumer organizations

UT_09_CS13

I would expect that agreements regarding appropriate levels and type of information as well as who has access and for what purpose and length of time would exist. I would also expect that no information could be used for sale or use without the permission of the individual.

Domain Information authorization and access controls

Stakeholder Consumers or consumer organizations

UT_09_CS14

Information should go to the person that it is intended for only. There should be a mechanism in place that can provide reasonable assurances that will occur. Sometimes it's the case that files are misplaced or a fax is mis dialed. There are several precautions that can be in place to mitigate these occurrences. (encryption, verification of sender/receiver, password protection)

Domain Administrative or physical security safeguards

Stakeholder Consumers or consumer organizations

UT_09_CS26

I would first check with my insurance to make sure that it was an appropriate benefit under my plan. Then I would call the doctor that wrote the prescription and have the office manager call the pharmacy to verify that it had been filled. I would follow up with a call to the pharmacy and check on the prescription myself.

Domain Information use and disclosure policy

Stakeholder Consumers or consumer organizations

Pharmacy Benefit - Scenario B

UT_10_01-1BP_business_agreements_share_patient_data_pharmacy

As a pharmacist, formal business associate agreements to share data are not needed to review data for proposal purposes as protected health information is not shared. Only data that is de-identified is shared and only that which is the minimum necessary for the review.

Domain Administrative or physical security safeguards

Stakeholder Pharmacies

Legal Driver § 164.514 Other requirements relating to uses and disclosures of protected health information. The minimum necessary rule would require that only de identified/aggregated information be provided if that is sufficient to carry out PBM1's assignment. 45 CFR 164.514(d) .If only de identified information is provided, HIPAA would not require a business associate agreement.

UT_10_01BP_business_agreements_share_patient_data_company

Our company has formal contracts in place with the pharmacy benefit managers that specifically state the terms and conditions under which data is exchanged and shared. These terms should include a disclosure by permission agreement only authorized between our company and the current pharmacy benefit manager (pbm); If our company wants to compare costs with another pharmacy benefit provider we can enter into an agreement with them to provide that information - a nondisclosure agreement between our company and the pbm that is doing a comparison assessment. Also, we would require a business associate agreement with the HIPAA privacy requirements between the company and the all pbm's involved.

Domain Administrative or physical security safeguards

Stakeholder Consumers or consumer organizations

Legal Driver Company A needs to enter in a business associate agreement with PBM1 if patient identifying information is to be used. The requirements of the business associate agreement are set forth in 45 CFR 164.504(e)(2); the business associate agreement would typically be worded to permit PBM1 to have access to relevant patient information only for the purposes of carrying out the specific assignment given by Company A.

UT_10_02-1BP_limits_on_info_shared__pharmacy

As the current PBM sending data to another PBM, even though the data would be de-identified, we would still provide the minimum amount necessary for an appropriate review. If the review would entail trending utilization on an individual employee basis, the data could be linked generically, such as Employee A, Employee B, etc.

Domain Information use and disclosure policy

Stakeholder Pharmacies

Legal Driver § 164.514 Other requirements relating to uses and disclosures of protected health information. The minimum necessary rule would require that only de identified/aggregated information be provided if that is sufficient to carry out PBM1's assignment. 45 CFR 164.514(d).

UT_10_02BP_limits_on_info_shared__company

From the company's perspective, any information shared should not initially include identifiable patient information. It should be quantifiable group (aggregate) information because that is all the pbm needs to correctly calculate their comparable cost structure.

Domain Information use and disclosure policy

Stakeholder Consumers or consumer organizations

Healthcare Operations and Marketing - Scenario A

UT_11_01BP_non-direct_marketing

Our integrated health care system has no process at this time for obtaining authorization from our customers because we do not market directly to them. If faced with a situation regarding lack of referrals to a new rehab center, brochures may be distributed based on non-condition related criteria.

Domain Information use and disclosure policy

Stakeholder Hospitals

UT_11_02BP_internal_information_sharing_integrated_health_delivery

We are a large integrated health delivery system with multiple facilities set up as a single covered entity under HIPAA for all provider type activities. As such, sharing information among our facilities and corporate offices for business activities does not require patient authorization.

Domain Information use and disclosure policy

Stakeholder Hospitals

UT_11_03BP_authorization_for_marketing_information

When the marketing department of our integrated delivery system plans to distribute a brochure to the individuals we would run a report of the required diagnoses by diagnosis-related group (DRG) to create a list of those patient names and demographic information needed for contact. If our admission paperwork did not specifically ask for consent for demographic information to be used by our corporation, then we would require our marketing department to obtain that consent from the patients prior to transfer of data.

Domain Information use and disclosure policy

Stakeholder Hospitals

UT_11_04BP_patient_information_for_marketing

As a small hospital we would not release medical information for the specific purposes of increasing revenue from that patient. This would be in violation of my understanding of the intent of the HIPAA statute. On the other hand, if the marketing was done to improve quality of care, perhaps by assessing patient satisfaction with care, or to identify concerns with the entire process of care, that would seem appropriate.

Domain Information use and disclosure policy

Stakeholder Physician groups

UT_11_05BP_third_party_release_for_marketing

If our critical access hospitals were asked to release information for third party marketing we would: (1) obtain written patient consent that discloses the intended use of the data; (2) refrain from releasing information for purposes that are not disclosed to the patient at the time patient consent was obtained; (3) establish the provider's ownership rights in the data; (4) define and limit the purpose for which the third party is being given access to the data; (5) limit the scope by which the third party may use, disclose, or distribute the data, or prohibit third party disclosure and/or distribution altogether; (6) restrict access to patient-identifying information, where there is a need for third-party access to patient identifiers; and (7) require indemnification by third parties for harm the provider suffers as a result of a breach of confidentiality.

Domain Information use and disclosure policy

Stakeholder Hospitals

Healthcare Operations and Marketing - Scenario B

UT_12_01-1BP_patient_information_use

Marketing directors at our hospital know the general parameters by which patient information can be used for marketing. When at any time there are questions, a marketing director can seek guidance from the CEO. If the activity is at all questionable, the marketing is forgone.

Domain Information use and disclosure policy

Stakeholder Hospitals

UT_12_01BP_patient_information_use

Our hospital shares patient information internally with other departments. We provide information to patients on new services or classes and instruction. Our hospital registration form has language that allows patients to choose to opt out of a mail list that provides information sent to their homes for specified services. We do not sell patient information to outside vendors.

However outside vendors can include information/samples in kits that go home with patients. Patients can choose to register should they decide, with the vendors mailing list in a proactive manner.

Domain Information use and disclosure policy
Stakeholder Hospitals

UT_12_02BP_patient_information_for_internal_marketing

The marketing department internally uses de-identifiable patient information internally typically for planning or reporting purposes. This is done through an internal hospital department called "Decision and support services." This department has access to all patient data for the purpose of reporting trend aggregate patient data.

Domain Information use and disclosure policy
Stakeholder Hospitals
Legal Driver § 164.514 Other requirements relating to uses and disclosures of protected health information. The "minimum necessary" rule in 45 CFR 164.514(d) applies to the interactions between physician, pharmacy, and/or PBM. If one of the parties requests from the other information not relevant to treatment, patient, or health care operations, this would generally be prohibited by HIPAA both because the minimum necessary rule would have been violated and because the interaction would no longer fit within the definition of treatment, payment, or health care operations. The different parties involved must limit the types of persons who receive the patient information as well as the types of patient information received.

UT_12_03BP_patient_information_use_external_mail_house

Our hospital marketing department transmits identifiable data directly to a mail house to conduct patient-centered educational or follow up mailings to our patients.

Domain Information use and disclosure policy
Stakeholder Hospitals

UT_12_04BP_business_agreement_third_party_marketing

Our hospital marketing department has a business associates agreement with the mail house to ensure confidentiality

Domain Administrative or physical security safeguards
Stakeholder Hospitals

UT_12_05BP_transmit_patient_info_to_mail_list

The hospital marketing department mail list is typically sent via a CD or electronic file over e-mail with instructions for one time usage and destruction of the file after use (this is a common practice for mail houses and they readily comply).

Domain Information transmission security or exchange protocols
Stakeholder Hospitals

UT_12_CS15

I have a very negative opinion of this - Don't think this should happen.

Domain Information use and disclosure policy
Stakeholder Consumers or consumer organizations

UT_12_CS16

As a patient entering a hospital to give birth I wouldn't want to be asked about giving permission/authorization when being admitted. There is too much going on to focus on what is being asked of the patient. It should be at discharge.

Domain Information authorization and access controls
Stakeholder Consumers or consumer organizations

UT_12_CS17

As a consumer I am concerned about the security of my information. No identifiable patient

information should be transferred anywhere. Only general aggregate data and statistics.
 Domain Administrative or physical security safeguards
 Stakeholder Consumers or consumer organizations

Bioterrorism event

UT_13_01BP_collect_information_bioterror_investigation

As the local public health department officer, I would collect information from the patient's physician including a patient history. I would also collect patient information from the lab.

Domain State law restrictions
 Stakeholder Public health agencies
 Legal Driver 26-23b-103. Mandatory reporting requirements — Contents of reports — Penalties. (1) (a) A health care provider shall report to the department any case of any person who the provider knows has a confirmed case of, or who the provider believes in his professional judgment is sufficiently likely to harbor any illness or health condition that may be caused by: (i) bioterrorism.

UT_13_02BP_notify_possible_exposure_to_state

As the state health agency, reports of anthrax exposure are submitted to the state by the local health department's organizational patient safety officer. It is unlikely that the local public health dept in adjacent county would be notified of the initial report. We, the state health agency, would notify CDC and FBI in real-time.

Domain State law restrictions
 Stakeholder Public health agencies

UT_13_03BP_coordination_bioterror_investigation_federal

Our federal law enforcement is involved once the doctor suspects anthrax and submits the test to the lab. From here, the notification takes on a life of its own. The lab, if specimen is positive, notifies the Laboratory Response Network (LRN) - the LRN confirms the sample is positive and it goes to the CDC. The doc is notified as is the state health department. At the same time, the notification of a positive test is sent to the Strategic Information Operation Center (SIOC). This is a major hub of notification- all agencies are notified from here of the result. When an event occurs we are notified by local agencies and sometimes by the state. Usually the state is on-site when we arrive. It's unclear to us who contacts the state but they are always there when an event similar to this occurs. Our role beyond investigative is to aid with the coordination of federal resources should more be necessary.

Domain State law restrictions
 Stakeholder Other Specified Law Enforcement

UT_13_04BP_coordination_local_bioterror_investigation

In the event of a bioterror investigation as local law enforcement we receive a general alert but nothing with detailed or specific information unless the threat was in the direct local area. We would identify or locate individuals and we would receive specific identifiable information on the person(s) involved along with direct instructions on how to proceed. Our instructions are going to come from the federal enforcement level and state health officials. For events that are not in our locality we would help to contain or secure an area.

Domain State law restrictions
 Stakeholder Other Specified Law Enforcement

UT_13_05BP_transmit_information

As local law enforcement officers we often deal with threat investigations and need to notify other agencies or organizations. Officers pick up the phone and call other organizations and will follow up with an email transmission of an "Urgent Report" that is sent electronically via email releasing only necessary information that will not compromise the investigation.

Domain Information transmission security or exchange protocols

Stakeholder Other Specified Law Enforcement

UT_13_06-1BP_public_release_of_information

As the state health agency we would not disclose the name of the patient or any other protected health information in the case of a suspected bioterror threat. Cases are handled on an individual basis - If anthrax is confirmed more information would likely be shared but the patient name is not disclosed.

Domain State law restrictions

Stakeholder Public health agencies

UT_13_06BP_public_release_of_information

Federal law enforcement release of information to the public during a coordinated investigative effort would be the responsibility of a joint unified command - this is made up of a representative from each head agency involved in the investigation.

Domain Information use and disclosure policy

Stakeholder Other Specified Law Enforcement

UT_13_CS18

I would gather information from the INTERNET, listen to the news, call my local doctor. Sometimes it feels as though we are living in a vacuum and there is a lack of information - this leads to disinformation - INTERNET blogs, chat rooms, talk radio - mostly people opinion spun with some fact. Really a real time national enquirer

Domain Information use and disclosure policy

Stakeholder Consumers or consumer organization

UT_13_CS19

Officials can release only that which is confirmed and it takes time to do that. Otherwise if information was released without caution it would be mass panic.

Domain Information use and disclosure policy

Stakeholder Consumers or consumer organizations

Employment Information Scenario

UT_14_01BP_generic_or_detailed_return_to_work_form

At our hospital, if the employee requests a generic release from our emergency room, there is usually no need for an authorization. If more detail is required by the requester, the provider discusses what MUST be included and documents patient authorization to release the information. In both cases the provider would talk with the patient and adhere to minimum standard under HIPAA, with regards to releasing information.

Domain Information use and disclosure policy

Stakeholder Hospitals

UT_14_02BP_patient_authorization_to_mail_or_fax_info

At our hospital if the employer will not accept hand carried documentation from the patient, we obtain a signed authorization from the patient and mail or fax the return to work form, verifying the employers contact information before sending the letter.

Domain Information use and disclosure policy

Stakeholder Hospitals

UT_14_03BP_Clarification_or_return_to_work_procedure

If a front line employee in our hospital were faced with this situation and was not familiar with our practices he/she would contact a supervisor or the compliance hotline for assistance. The practice of cutting and pasting information directly from an Electronic Health Record (EHR) would not occur at our ED.

Domain Administrative or physical security safeguards

Stakeholder Hospitals

UT_14_04BP_Information_included_in_generic_return_to_work
 Our hospital return to work letter contains the patient’s name, the physician’s name, the length of time under the physician’s care for the given illness, and any activity restrictions.

Domain Information use and disclosure policy
 Stakeholder Hospitals

UT_14_05-1BP_transmission_of_return_to_work_by_email_not_allowed
 In our hospital most “return to work” documents are either prepared and handed to the patient when they are present, or are mailed as needed. We do not share PHI with employers over the Internet.

Domain Information transmission security or exchange protocols
 Stakeholder Hospitals

UT_14_05BP_transmission_of_return_to_work_by_encrypted_email_with_partners
 Our hospital does currently permit sending encrypted e-mail messages with PHI to regular business partners, however, e-mail should not be used, regardless of whether it is encrypted, for communicating with patients or others.

Domain Information transmission security or exchange protocols
 Stakeholder Hospitals

UT_14_06BP_HR_Company_process_return_to_work
 In our company the general process for return to work is: He/she would be given a form from the medical provider stating that the person was now under medical care and it would state the length of time the person would need to be gone. It would most likely have only limited information as to the cause of the medical situation. It would be signed and dated by the appropriate person/institution so the employee could give it to their employer as justification for their absence from work. When an employee is off work for four days and is ready to return, we require them to bring (on first day) a Return to Work Release.

Domain Information use and disclosure policy
 Stakeholder Professional associations and societies

UT_14_07-1BP_Company_transmission_return_to_work_practice
 In our company the work release form must be given to the employee, signed and dated by her provider, so she can bring it with her or she will not be allowed to return to work.

Domain Information transmission security or exchange protocols
 Stakeholder Professional associations and societies

UT_14_07BP_Company_transmission_return_to_work_practice
 If our HR department were receiving a form by fax or email, the provider of the info would be responsible to determine the name/position of the person authorized to receive the info. Then if they were faxing it I would tell them to call me at the time they planned to fax, and I would stand at the fax to receive it. If it is email, I would give them my direct email and then it is still their responsibility to determine the security protocols at their end, for safe data transmittal. The safest way is mail.

Domain Information transmission security or exchange protocols
 Stakeholder Professional associations and societies

UT_14_08BP_HR_dept_receipt_of_unrequested_info
 Our HR department would put the un requested information in an envelope and give it to the employee with an explanation that it had come to us un-requested and therefore I would turn it over to the employee. I would remind them that we still require the basic information for their return to work and they would be expected to provide that.

Domain Information transmission security or exchange protocols

Stakeholder Professional associations and societies

UT_14_CS20

Review the portion of the Electronic Health Record (EHR). If there were items that I was uncomfortable sharing I would ask the doctor for a release "return to work" instead.

Domain Information use and disclosure policy

Stakeholder Consumers or consumer organizations

UT_14_CS21

With Electronic Health Record (EHR) record no copy is obtained by consumer/patient, unless specifically requesting a copy. The patient is left out of this process.

Domain Information authorization and access controls

Stakeholder Consumers or consumer organizations

UT_14_CS22

Individuals receiving ELECTRONIC HEALTH RECORD (EHR) may or may not have access to that type or level of personal information. If I chose the ER, I would have to request that information and provide an email address for my HR rep.

Domain Information authorization and access controls

Stakeholder Consumers or consumer organizations

Public Health - Scenario A

UT_15_01BP_clinician_notify_public_health

As a physician, I would report the case of confirmed active TB to the Public Health Department. Our Notice of Privacy Practice indicates we reserve the right to use any and all patient information to identify the patient with the Public Health Department in such situations. The Director of Nursing would be the responsible person initiating the contact. A fax with any information necessary would be distributed given this is acceptable.

Domain Information use and disclosure policy

Stakeholder Clinicians

UT_15_02BP_departing_state_notify_arriving_state

As the Public Health Department in the state patient was departing from, we would first contact the other state to meet the bus so all travelers could be treated. Typically, if there is a public health threat, we phone confirming that a fax is coming and then we fax confidential information.

Domain State law restrictions

Stakeholder Public health agencies

UT_15_03BP_departing_state_notify_bus_company

As the Public Health Department in the state the patient was departing from, we would try to get the manifest from the bus company so we could contact travelers that may have departed the bus prior to final destination (we may need to divulge the TB info but not the individual's name). If any passengers exited the bus in our state we could transport them to a secure TB unit and would proceed to secure court orders for treatment.

Domain State law restrictions

Stakeholder Public health agencies

UT_15_04BP_arriving_state_notify_law_enforcement

As the Public Health Department in the state where patient was traveling to, we would provide a temporary order. This would require law enforcement involvement. We would share the order with law enforcement but no other information would be shared.

Domain State law restrictions

Stakeholder Public health agencies

UT_15_05BP_law_enforcement_notified

As law enforcement, the Public Health Department notifies us that an individual is a threat to the public. For Law Enforcement to get involved we would need official paperwork in the form of a subpoena (warrant, declared state of emergency, imminent public threat) in order to act. Public Health would need to initiate the order and then we would supply the muscle. Without the paperwork, Law Enforcement has no legal jurisdiction. In reality our communication channels are not well established at the local level for this type of effort. We receive no additional information beyond what is provided in the order regarding health dangers to officers on the scene.

Domain State law restrictions
Stakeholder Other Specified Law Enforcement

UT_15_CS23

It is expected that the primary care physician inform patients that fall under the condition/disease notification requirements, what information is to be shared, by whom, and under what conditions. If I had not been informed I would be infuriated to find out that my health information had been shared with an untold number of individuals and agencies. Even if informed, instructions would need to be very specific and easy as opposed to just call the Health Department. This would probably lead to endless frustration and wading through front line staff trying to locate the right person or program.

Domain Information use and disclosure policy
Stakeholder Consumers or consumer organizations

UT_15_CS24

I would submit hard copies of health information in person. I wouldn't trust email or fax to be confidential. Plus based on this experience, I'd ask what their agency's policy is regarding records handling, retention, confidentiality, and destruction.

Domain Information transmission security or exchange protocols
Stakeholder Consumers or consumer organizations

Public Health - Scenario B

UT_16_01BP_testing_by_reference_lab

As a reference lab manager, we receive test orders and specimens from the State Health Laboratory over a laboratory information system interface. Some limited demographic information is associated with the order. Test results are returned over the same interface. We do not directly notify the physician or patient regarding results and we do not receive orders directly from physicians.

Domain Information transmission security or exchange protocols
Stakeholder Laboratories

UT_16_02BP_abnormal_result_process

As the newborn screening unit at the state lab, we would notify the state follow up program of the abnormality. We would proceed with a second test to confirm the abnormality.

Domain State law restrictions
Stakeholder State government

UT_16_03BP_transmission_lab results

All abnormal results obtained from us (newborn screening unit - state lab) are called to the Medical Home. Verbal information is given including symptoms. A letter detailing the abnormality, needed follow up, and including symptoms is faxed or mailed to the Medical Home. The mailer (results) include a detailed description of the results and symptoms.

Domain State law restrictions
Stakeholder State government

UT_16_04BP_state_public_health_access_to_patient_information

As the state public health department, we have legal access to all of the identifying information for state mandated programs.

Domain State law restrictions

Stakeholder State government

UT_16_05BP_State_public_health_notify_parents

As the health department, our appropriate state program would notify the patient's parents that they are eligible for services and leave a contact number for them with a copy also going to the medical home/ physician in case we have an old address for the patient.

Domain Information use and disclosure policy

Stakeholder State government

UT_16_06BP_physician_office_health_dept_communication

In our physician office, information about patients is received by my nurse from the health department. She then informs me. If I need to let the health department know information I inform my nurse and she calls the health department. (i.e. positive flu test).

Domain Information use and disclosure policy

Stakeholder Clinicians

UT_16_07BP_physician_contact_parents_with_results

As the physician, I would inform the patient's parents that their child has this disease. I would also let them know that the state lab would be tracking the health of their child and that there would be services available through the state.

Domain State law restrictions

Stakeholder Physician groups

Public Health Scenario C

UT_17_01-1BP_health_information_sharing_between_facilities

As the physician from a clinic that serves homeless persons information can be shared freely among all caregivers unless a counselor is discussing some private/legal abuse issues.

Domain Information use and disclosure policy

Stakeholder Clinicians

UT_17_01BP_health_information_sharing_between_facilities

As a not for profit treatment facility who treat homeless, we share with some frequency a predetermined set of patient data with other agencies. The agencies often don't want more, because it has limited utility. Our data is shared with the county programs as defined by contract. When we are functioning as a shelter situation the data sharing is limited in that we will only respond to requesting agencies that the client has entered into treatment.

Domain Information use and disclosure policy

Stakeholder Community clinics and health centers

UT_17_02BP_homeless_shelter_receiving_request_for_PHI_from_public

As homeless shelter staff, under the original signed consent form, the case manager would notify the authorized drug treatment staff that a relative is attempting to locate the client. The treatment staff could then pass this information on to the client who could then, at their own discretion, contact the inquiring relative. This would assume a broad interpretation of CFR 42 Part II, because technically the federal regulation governing substance abuse treatment information restricts the disclosure to information specified in the original release.

Domain Information use and disclosure policy

Stakeholder Community clinics and health centers

UT_17_03-1BP_release_of_PHI_to_possible_relative

As a drug treatment center, we would neither “confirm nor deny” the participation of any client residing at the treatment.

Domain Information use and disclosure policy

Stakeholder Community clinics and health centers

UT_17_03BP_release_of_PHI_to_possible_relative

As a primary care provider I would not release any medical or other information to any person claiming to be a relative without that patient’s knowledge and a release of records/information signed by that patient. The release of information would have to be specific pertaining to the information being exchanged.

Domain Information use and disclosure policy

Stakeholder Clinicians

UT_17_CS25

I understand and appreciate the reluctance on part of the homeless shelter to release information regarding my relative, especially since I did not have proper identification. I would hope, however, that instead of being turned away I would be provided with the proper steps to take in order to contact my relative and see if they are indeed okay.

Domain Information use and disclosure policy

Stakeholder Consumers or consumer organizations

State Government Oversight

UT_18_01BP_pediatrician_lead_screen

As a pediatrician I screen for risk of lead poisoning at the 1 year well-baby check appointment. I probably should be checking at the two-year check as well. However I have not yet seen a positive lead lab result. It doesn’t seem to be an issue here.

Domain State law restrictions

Stakeholder Clinicians

UT_18_02BP_lab_submit_positive_lead_result_to_state

As the lab that is contracted to conduct the blood lead lab tests for the state, we notify electronically the appropriate program manager at the state health department on a weekly basis. If there are elevated levels we notify immediately. The secure file transfer is accessible by password. Our lab places an excel spreadsheet on our secure site and the state program manager can download the file to their system electronically. Utah does not require a universal blood lead testing for children.

Domain State law restrictions

Stakeholder Laboratories

UT_18_03BP_establishing_data_sharing_agreement_Public_Health_to_University

As a data steward responsible for immunization data in the Department of Health, before we would share any data, we would establish data sharing agreements with the university and then have these agreements reviewed by our legal department prior to obtaining signatures.

Domain State law restrictions

Stakeholder State government

UT_18_04BP_university_researcher_access_to_data

As a data steward responsible for immunization data in the Department of Health, if a researcher from the university had a legitimate need to access data in the state immunization database, they would go through the enrollment process and fill out all the required paperwork

(confidentiality forms, user security agreement, etc.). Then, after training, they would be granted access but restricted to “look up only” so no alterations to information could be done.

Domain
Stakeholder

State law restrictions
State government

Appendix D.

Work Group Members

Appendix D. Project Work Group Members

Steering Committee

Chair

Joseph G. Cramer, MD
Cottonwood Pediatrics
Murray, UT

Rulon Barlow
Orem, UT 84058

Scott Barlow, CEO
Central Utah Clinic
Provo, UT

Terry Holmes
TelNetZ, Inc.
Draper, UT

Michael Jensen
Blanding, UT

Bradley LeBaron
CEO/Administrator
Uintah Basin Medical Center
Roosevelt, UT

Deb LaMarche
Utah Telehealth Network
Salt Lake City, UT

R. Chet Loftis
Salt Lake City, Utah

Dennis Moser, FACHE
Utah Center for Rural Health
Cedar City, UT

Mark A. Munger, PharmD
University of Utah
Salt Lake City, UT

Barry Nangle, PhD
Director, Center for Health Data
Utah Department of Health
Salt Lake City, UT

Rod Ross
Equitable Life & Casualty Insurance
3 Triad Center
Salt Lake City, UT

John Nelson, MD
Medical Director
HealthInsight
Salt Lake City, UT

Linn J. Baker, Director
Utah's Public Employees Health Program
Salt Lake City, UT

Lyle Odendahl, JD
Assistant Attorney General
Salt Lake City, UT

Thomas Jackson, VP Operations
HealthInsight
Salt Lake City, UT

Lois Haggard, PhD
Director, Office of Public Health Assessment
Utah Department of Health
Salt Lake City, UT

Variations Work Group

Chair:

John Nelson, MD
Medical Director
HealthInsight
Salt Lake City, UT

Kim Batemen, MD
Central Utah Practitioner
Salt Lake City, UT

Kevin M. Coonan, MD
Adjunct Assistant Professor
Division of Emergency Medicine
NLM Fellow, Department of Medical Informatics
University of Utah School of Medicine
Salt Lake City, UT

Katie Gorris
Privacy Office, Intermountain Healthcare
Salt Lake City, UT

Reid L. Barker
Executive Director
Utah Pharmaceutical Association
Orem, UT

Sara V. Sinclair RN
Chief Executive Officer
Sunshine Terrace Foundation, INC
Logan, UT

Jan Root, PhD
Assistant Executive Director
Utah Health Information Network
Murray, UT

Detective Von Steenblik
Centerville Police Department
Centerville, Utah

Appendix D. Project Work Group Members

Dr. Robert P. Huefner
Professor of Political Science
University of Utah
Salt Lake City, UT

Linda Johnson RN
Project Coordinator
HealthInsight
Salt Lake City, UT

Lois Haggard, PhD
Director, Office of Public Health Assessment
Utah Department of Health
Salt Lake City, UT

Allan D Ainsworth, PhD
Executive Director, Fourth Street Clinic
Salt Lake City, UT

Legal Work Group

Chair:
Lyle Odendahl, JD
Assistant Attorney General
Salt Lake City, UT

Liz Winter, JD
Deputy General Counselor
University of Utah
Salt Lake City, UT

Rex Olsen, JD
Assistant Attorney General
Utah Department of Health
Salt Lake City, UT

Morris Linton, JD
Senior Counsel
Intermountain Healthcare
Legal Department
Salt Lake City, UT

R.Chet Loftis, JD
Kirton & McConkie
Salt Lake City, UT

Solutions Work Group

Chair:
Linn J. Baker
Director
Utah's Public Employees Health Program
Salt Lake City, UT

David Call
Vice President
Deseret Mutual Benefit Administrator
Salt Lake City, UT

Kevin M. Coonan, MD
Adjunct Assistant Professor
Division of Emergency Medicine
NLM Fellow, Department of Medical Informatics
University of Utah School of Medicine
Salt Lake City, UT

Grant Howarth
President/CEO
Community Nursing Services
Midvale, UT

Jan Root, PhD
Assistant Executive Director
Utah Health Information Network
Murray, UT

Christie Chesler
TB Control/ Refugee Health Program Manager
Utah Department of Health
Salt Lake City, Utah

Dan Anderson
Legal Counsel
PEHP
Salt Lake City, UT

Dr. Larry V. Staker MD
Medical Director
Deseret Mutual Benefits Association
Salt Lake City, UT

Bob Rolfs, MD
State Epidemiologist
Utah Department of Health
Salt Lake City, UT

Iona Thraen
Patient Safety Director
Utah Department of Health
Salt Lake City, UT

Detective Von Steenblik
Centerville Police Department
Centerville, Utah

Dave Valenti, MD
American College of Emergency Physicians (ACEP)
Salt Lake City, UT

Implementation Planning Work Group

Chair:
Barry Nangle, PhD
Director, Center for Health Data
Utah Department of Health
Salt Lake City, UT

Appendix D. Project Work Group Members

Val Batemen, MBA, MHA
Executive Vice President
Utah Medical Association
Salt Lake City UT

Richard Melton, PhD
Deputy Director
Utah Department of Health
Salt Lake City, UT

Jan Root, PhD
Assistant Executive Director
Utah Health Information Network
Murray, UT

Lyle Odendahl, JD
Assistant Attorney General
Salt Lake City, UT

Mark Brinton, JD
Utah Medical Association
Salt Lake City UT

Kevin M. Coonan, MD
Salt Lake City, UT

Katie Gorris
Privacy Office, Intermountain Healthcare
Salt Lake City, UT

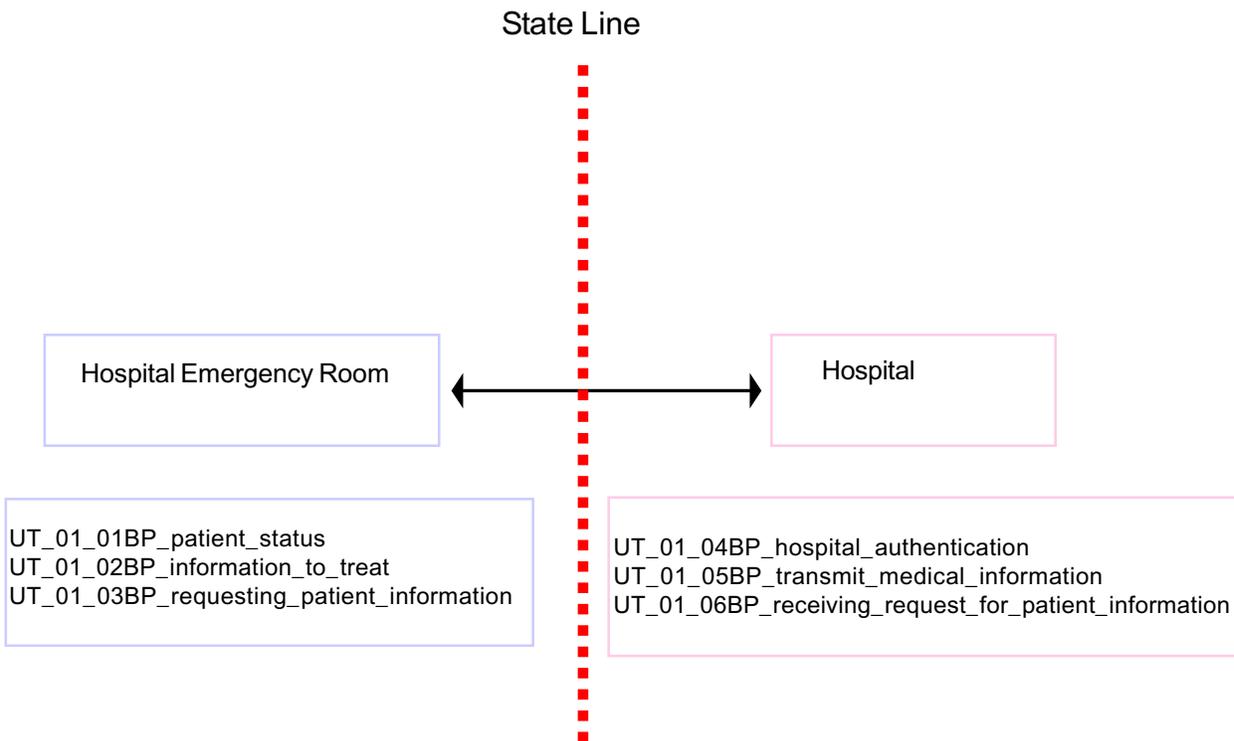
Lois Haggard, PhD
Director, Office of Public Health Assessment
Utah Department of Health
Salt Lake City, UT

Appendix E.

Scenario Maps

Appendix E. Business Practice Map by Scenario

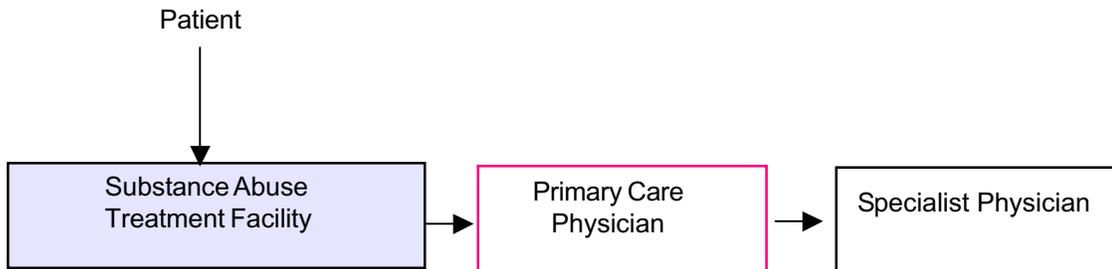
Patient Care A



Observations: When an emergency room physician is dealing with an emergency situation and needs patient's medical information the physician will make efforts to access the patient's medical information without patient authorization. In an emergency situation hospitals will disclose information without authorization to a requesting covered entity once that entity is verified. The release of patient information across state lines was a factor in the exchange of patient information.

Appendix E. Business Practice Map by Scenario

Patient Care B



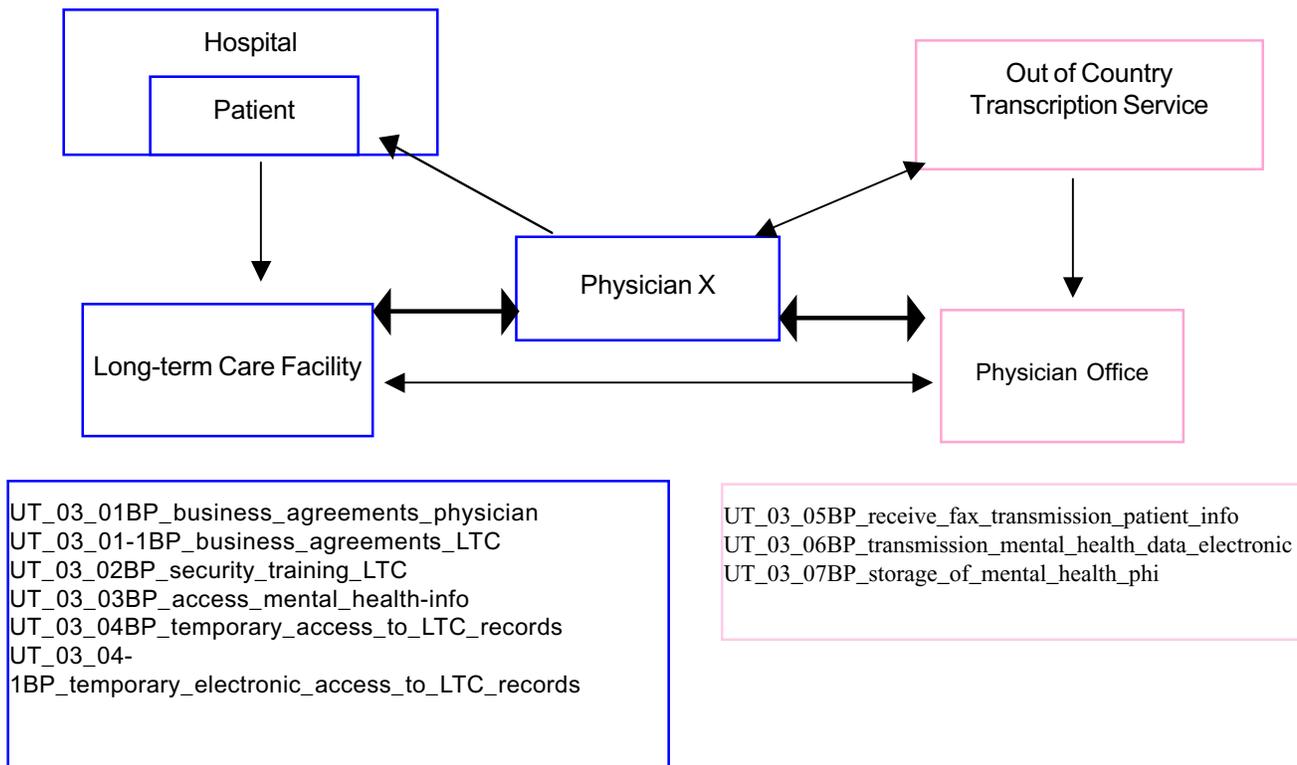
UT_02_01BP_patient_authorization
UT_02_01-1BP_patient_authorization_to_release_PCP_to_SPEC
UT_02_01-2BP_patient_authorization_to_release_PCP_to_SPEC
UT_02_02BP_determining_information_to_be_sent
UT_02_03BP_facility_authenticating
UT_02_04BP_transmission_non-electronic_SA to PCP
UT_02_05BP_transmission_electronic_SA to PCP
UT_02_05-1BP_transmission_PCP to SPEC
UT_02_06BP_verifying_receipt_of_record

UT_02_07BP_logging_disclosures
UT_02_08BP_recording_access_to_SA_PHI
UT_02_09BP_storage_of_SA_PHI
UT_02_09-1BP_storage_of_SA_PHI_restricted_access
UT_02_10BP_patient_consent_to_treat_PCP

Observations: There are differences between how a provider uses and discloses patient medical information when substance use is involved. There is variation among treatment facilities, physicians', and integrated delivery systems understanding of C.F.R 42 Part 2, it's relation to HIPAA, and the application of each. Treatment facilities note stringent precautionary measures to safeguard patient substance use information. While physicians comment on limited or restricted access to patient medical files and often choose not to request those records because of the perceived difficulties in access and use. Treatment facilities note that patient substance files are specially protected and kept in a locked cabinet behind a double locked door.

Appendix E. Business Practice Map by Scenario

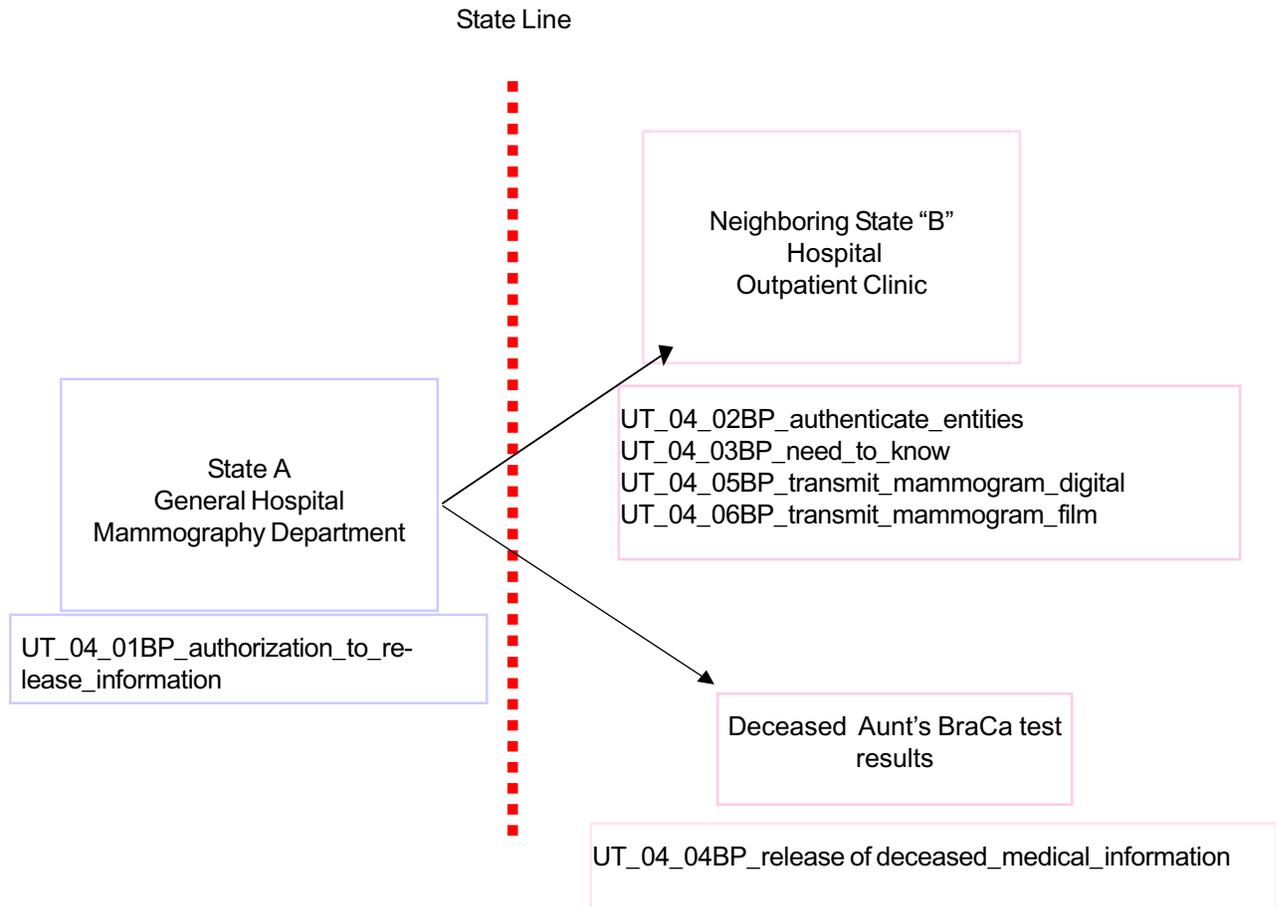
Patient Care C



Observations: There is variation among long-term care facilities practices for granting physicians temporary access to their facility and records system but facilities have procedures in place should temporary access be necessary under such situations. The sharing of patient information differs from provider to provider with some requiring that a business associate agreement be in place and others indicating such agreements are not necessary between providers involved in the treatment of a patient. Most information transmitted to and from long-term care facilities is done by fax.

Appendix E. Business Practice Map by Scenario

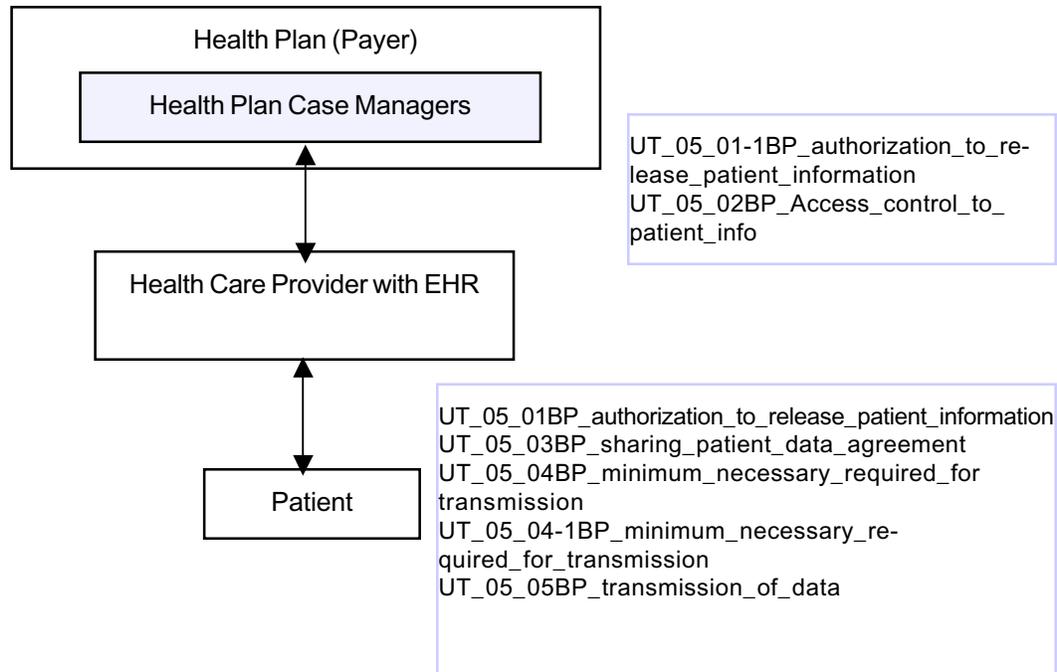
Patient Care D



Observations: The majority of mammograms done in our state are on film; this is the case in both rural and urban facilities. One Integrated Delivery System (IDS) currently uses digital images for mammography and a second has plans to transfer to digital within the next two years. However, even at the IDS that uses digital, the images are printed in hard copy for the physicians as most institutions and physicians are not comfortable with digital. Films are transmitted or exchanged by mail, courier, or the patient with signed patient release. There is no implication for exchanging information across state lines or when dealing with an HIV positive patient as precautionary measures would not differ given this condition. Requests from out of state facilities require authorized release that is faxed or mailed. Utah Code 78-25-26 establishes regulations for release of medical information for a deceased relative.

Appendix D. Business Practice Map by Scenario

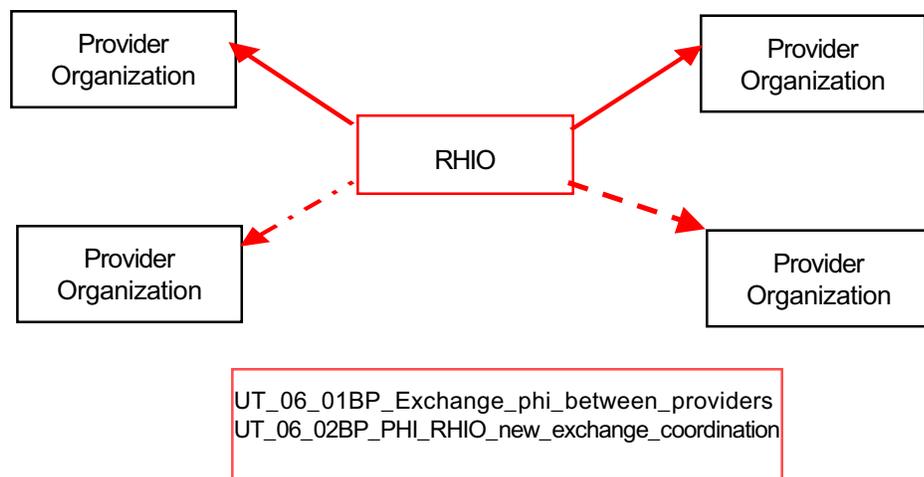
Payment



Observations: Payers work with the understanding that authorization is not needed for payment purposes. Nevertheless, payers will engage in business agreements with health care providers to facilitate the payment process. Health care providers show variation in whether or not they obtain authorization from patients to allow access to patient information for payment purposes. Providers tend to error on the side of caution and more often will obtain patient consent. As providers have different levels of EMR technology and comfort with this technology the process by which payers accesses patient and billing information varies. Both payers and providers report little variation in the description of what constitutes “minimum necessary” according to HIPAA.

Appendix E. Business Practice Map by Scenario

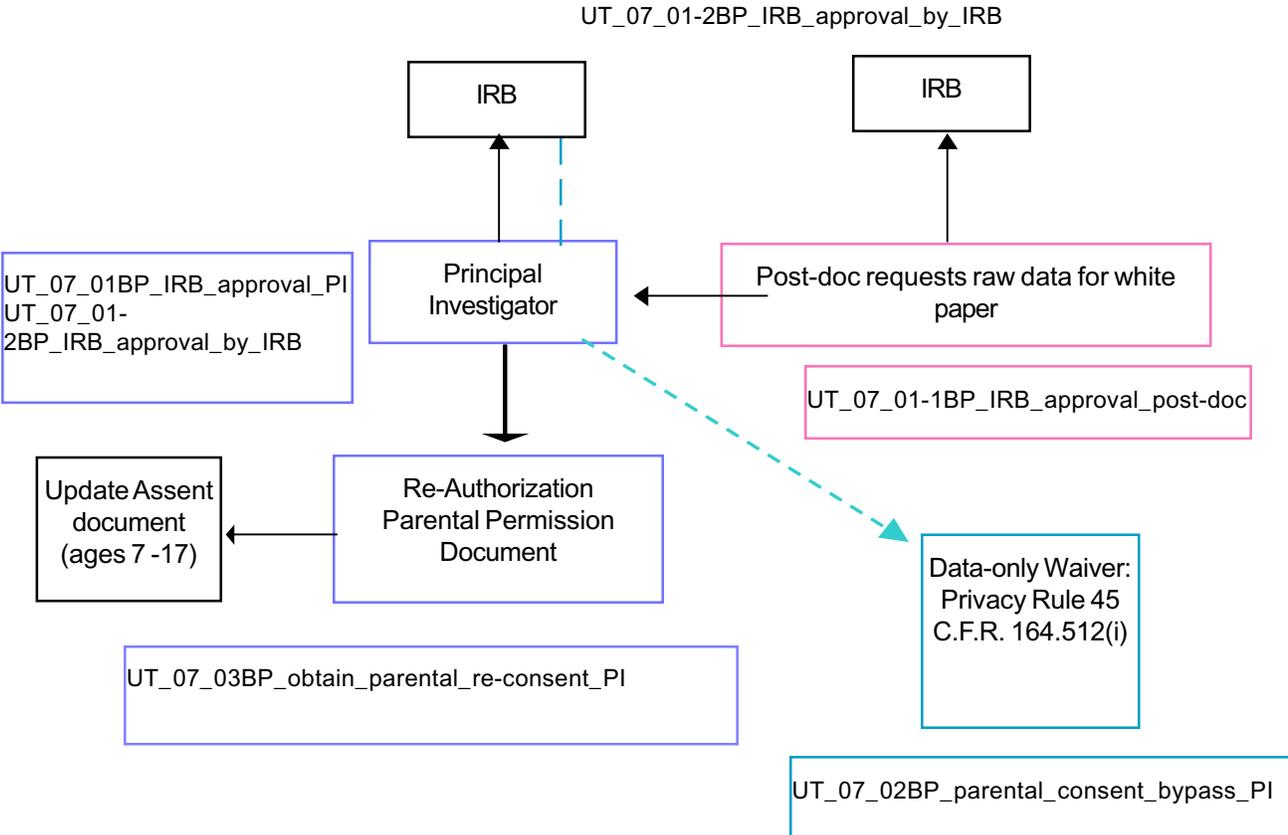
Regional Health Information Organization (RHIO)



Observations: The RHIO scenario does not describe the services performed by the Utah RHIO. The Utah RHIO is a gateway or information highway where information is exchanged between different organizations. The Utah RHIO does not request or permanently store data. The Utah RHIO functions like the post office in getting information routed from the sender to the intended receiver. The Utah RHIO does not perform quality measurements on its member's data. The Utah RHIO has a standards committee for chartering a subcommittee to develop a community standardized message should members want to exchange/submit patient information from one organization to another.

Appendix E. Business Practice Map by Scenario

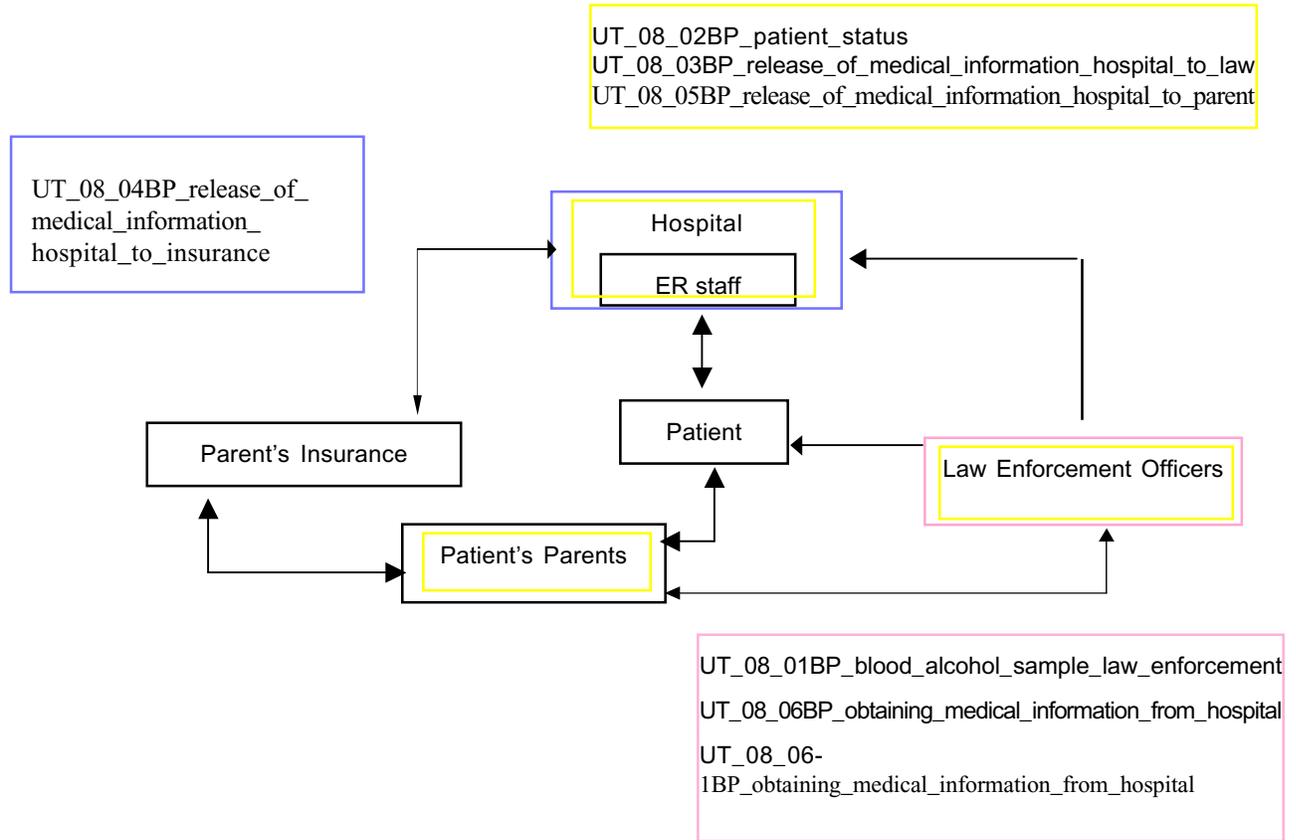
Research Data Use



Observations: The decision to resubmit to IRB is found to be at the discretion of the principal investigator, variation exists in this decision. Even though it is implied that the drug company owns the data the decision to resubmit is linked to authorship. If the principal investigator does not want to have ties to the secondary analysis he/she will request the post-doc to independently submit to IRB. Variation is noted in the requirement of parental approval for the use of data beyond that originally included in the protocol approved by IRB. Some believe the approval is required and others believe it can be waived.

Appendix E. Business Practice Map by Scenario

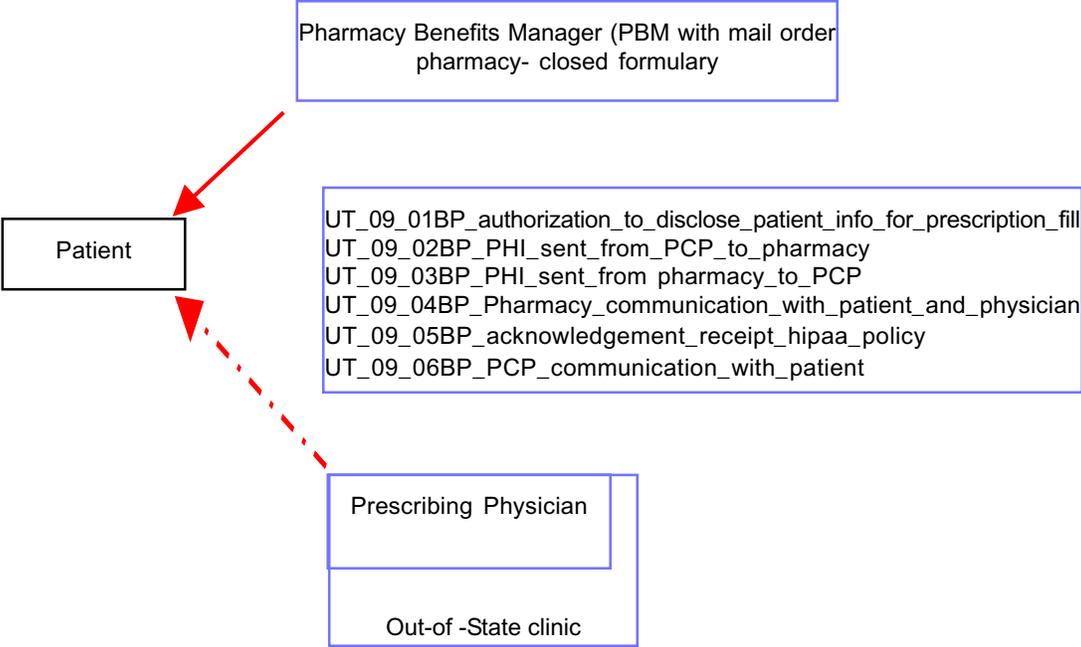
Access by Law Enforcement



Observations: A chasm exists between law enforcement and hospital with regards to communication. Hospital physicians are not willing to disclose information without subpoena to avoid legal entanglements. Hospital physicians are also very careful not to disclose information to parents and instead will opt to let the patient inform parents regarding their medical information. No agreements between law enforcement and hospitals for blood alcohol levels. Most law enforcement agencies have business agreements with paramedics for blood alcohol draws. Law enforcement officers are careful to gather as much information as possible before the patient gets to the hospital. Because little if any information can be gathered after the patient enters the hospital without initiating legal paperwork.

Appendix E. Business Practice Map by Scenario

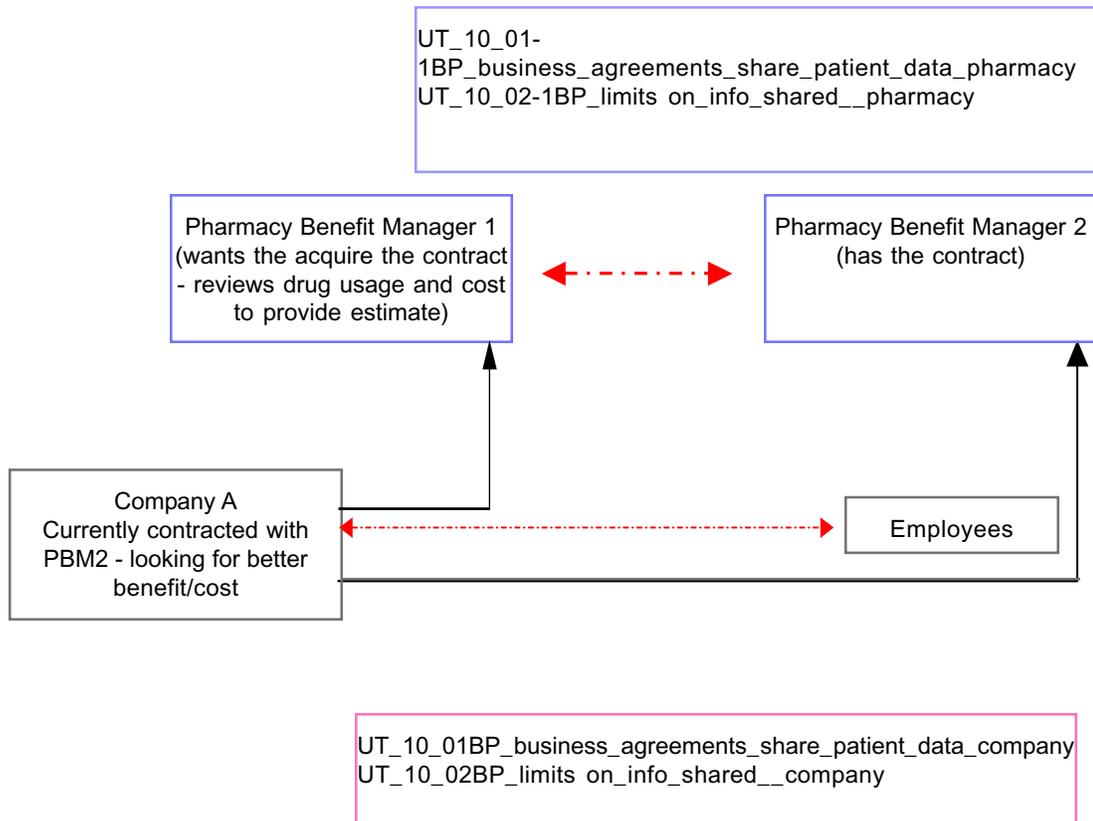
Pharmacy Benefit Manager A



Observations: There is variation in who contacts the patient to inform that the original prescription authorized is not on the formulary. In some cases the mail order pharmacy will contact the patient and in other cases it is the physician. Variation was reported in the options offered to the patient given this situation (e.g. pay out of pocket for original medication or choose an alternate medication). Consistent agreement that pharmacy receives “minimum necessary” to fill their orders.

Appendix E. Business Practice Map by Scenario

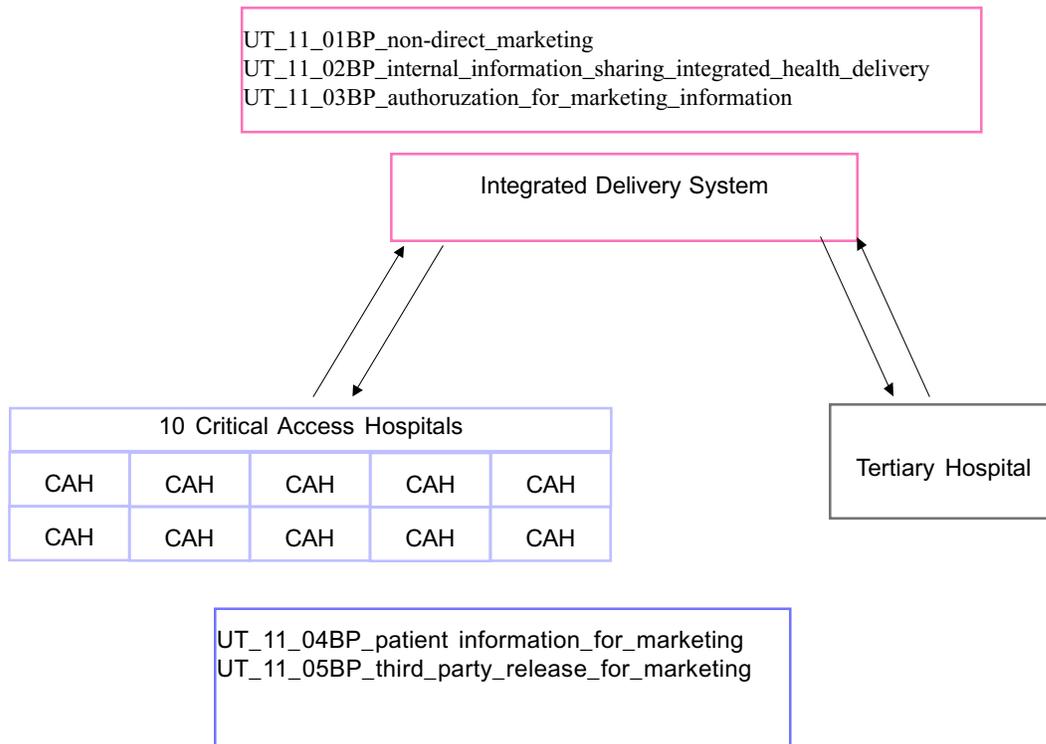
Pharmacy Benefit Manager B



Observations: Variation exists in whether or not a business agreement is required to share information between the parties. The company reported they would require a business associates agreement regardless of whether the data was de-identified. The pharmacy benefits manager did not feel an agreement was necessary if the data was a de-identified.

Appendix E. Business Practice Map by Scenario

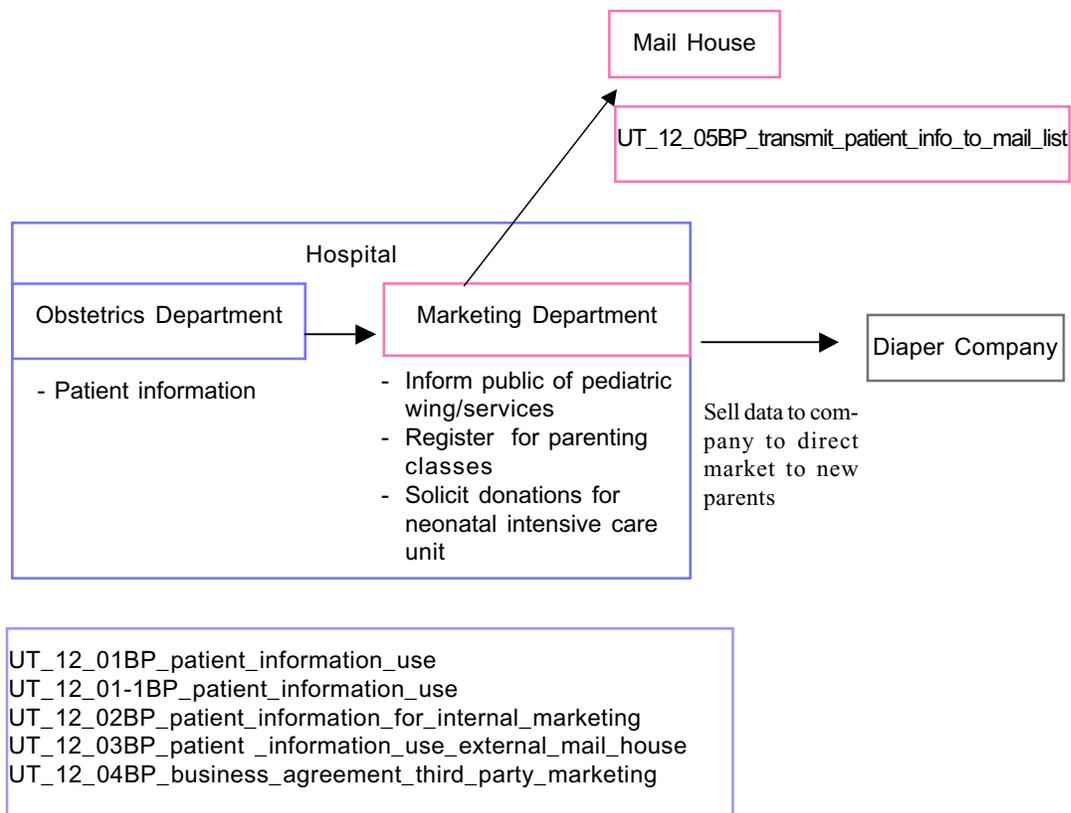
Healthcare Marketing and Operations A



Observations: This scenario is not very applicable in Utah. Not many entities, if any, were found to market in this fashion. These entities rarely direct market to individuals. General brochures are a more common form of marketing in Utah as concerns were expressed about HIPAA and the use of PHI to generate revenue. In the case that covered entities would direct market, patient authorization would be required.

Appendix E. Business Practice Map by Scenario

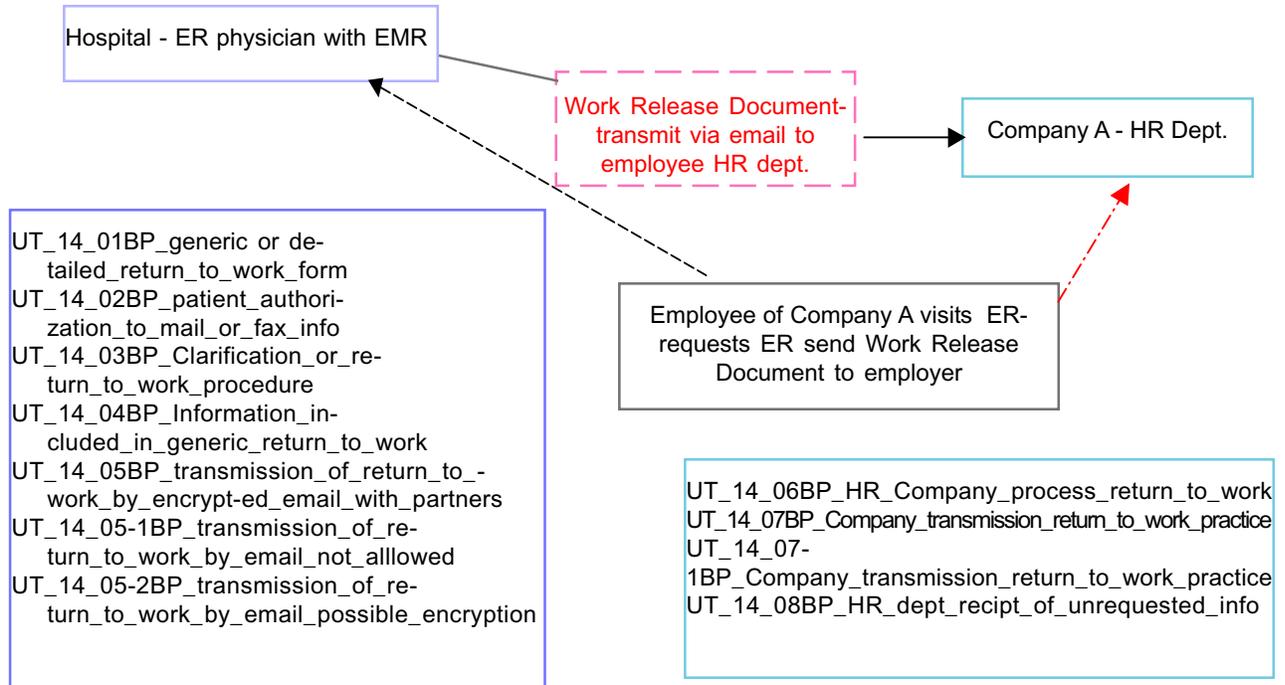
Healthcare Marketing and Operations B



Observations: One hospital system reported having a business agreement with a mail house that specifies the terms and limits of the contract for direct mailing. The hospital provides PHI on CD or electronic file to the mail house that is for one time use and then destroyed. We found no selling of PHI to outside entities. Different hospitals use PHI in different ways for marketing purposes. Some use the mail house as outlined above and others have an internal marketing department that sends information out. If the marketing is done internally the data is de-identified.

Appendix E. Business Practice Map by Scenario

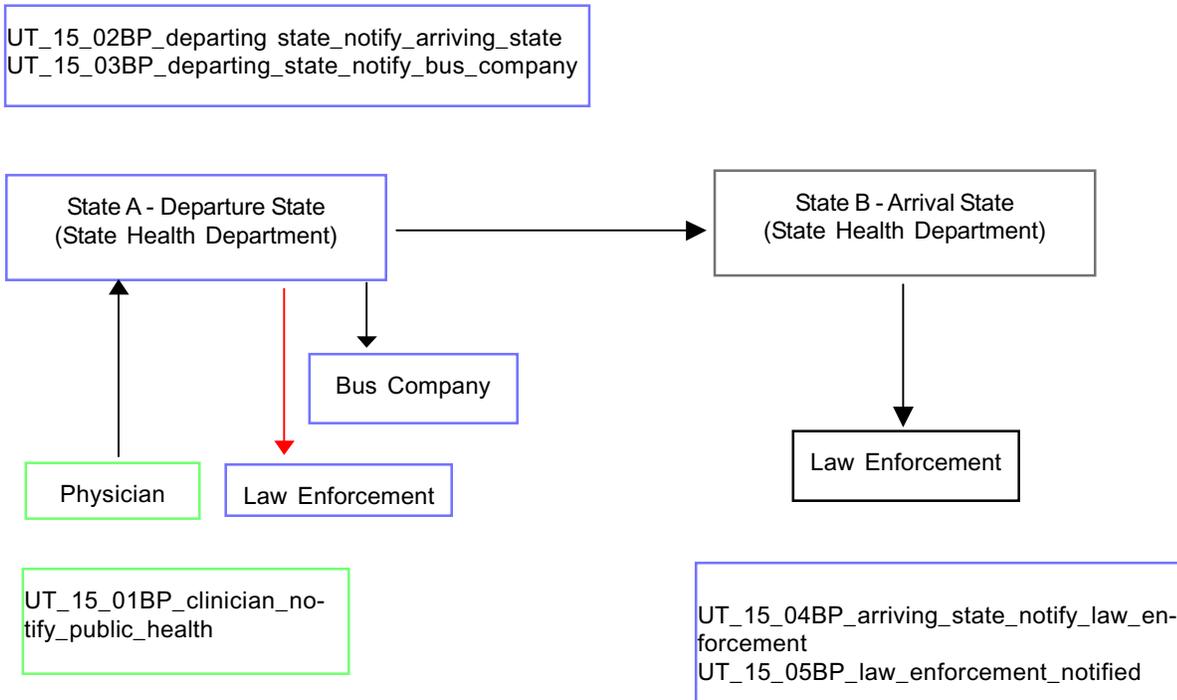
Employee Healthcare



Observations— We found that no hospital transmits info via email from their EMR systems for return to work purposes, nor did any feel this was appropriate. Minimum necessary under HIPAA is critical in this scenario.

Appendix E. Business Practice Map by Scenario

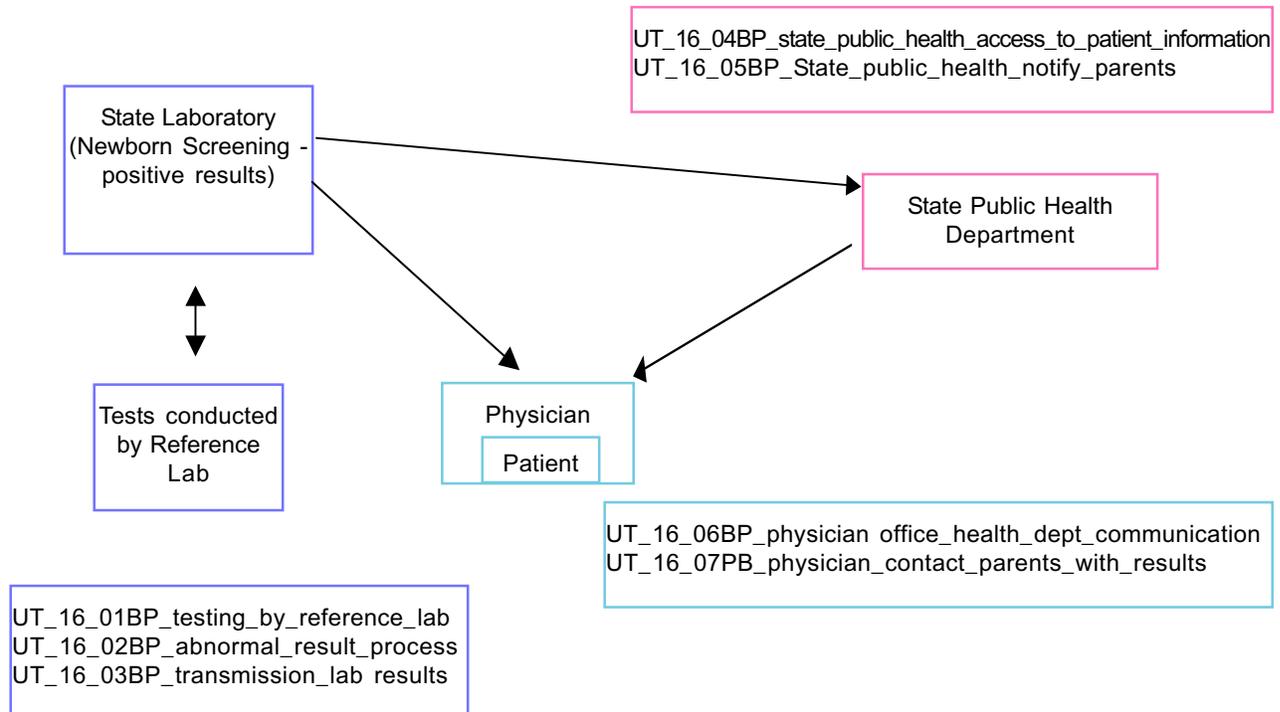
Public Health A



Observations: Poor communication channels between local law enforcement and public health. Information flows in one direction. Law enforcement enters situations without all information necessary to appropriately protect their officers. The state has resources like a secure TB unit in case of this type of emergency. The state has a policy to balance individual liberty interest with the need to protect the public health through quarantine in the event of a mass exposure to a harmful biologic agent (Policy Utah Code 26-6b).

Appendix E. Business Practice Map by Scenario

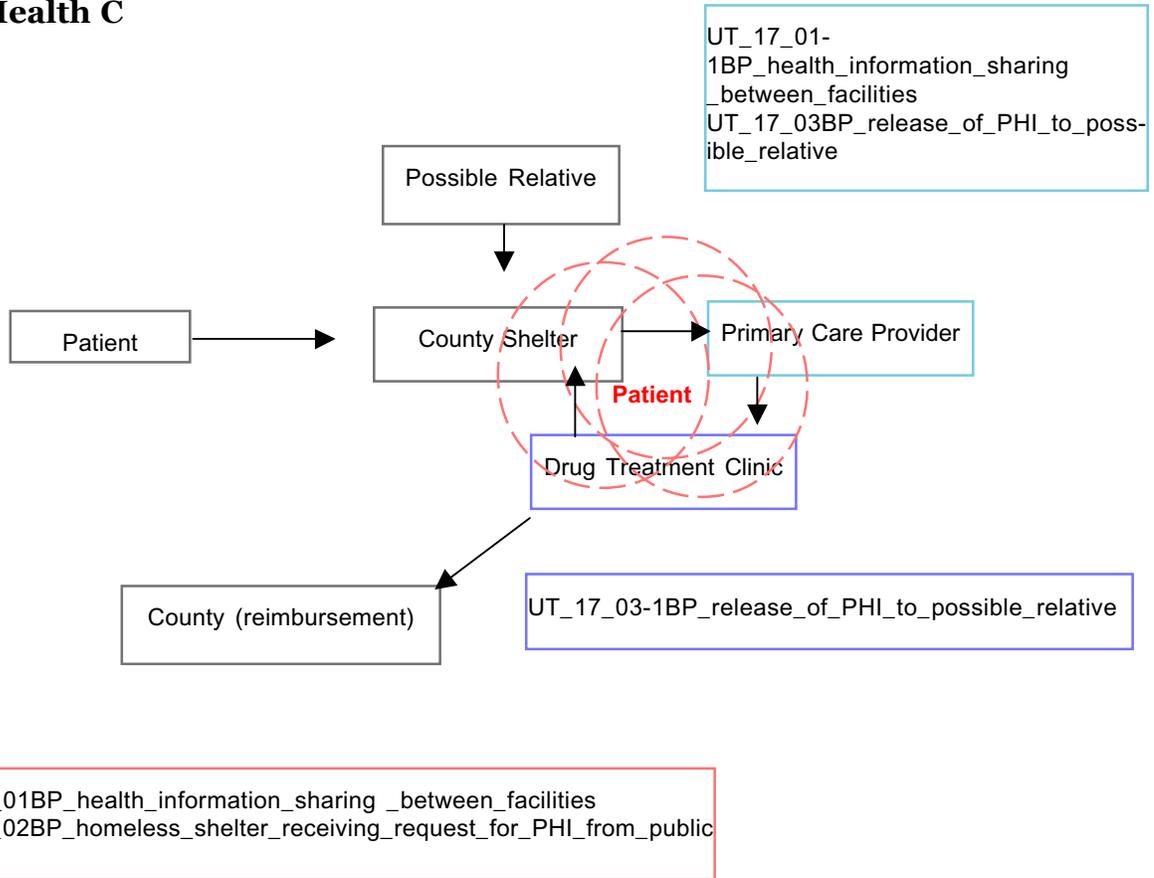
Public Health B



Observations: 1) Utah does not notify the specialty care centers unless there is critical (as agreed upon when establishing the follow up protocol for each disorder with the specialists) results. We do not have or use an Interactive Voice Response System. We do not have a registry for our identified and confirmed cases. Identified PKU and galactosemia (gg and Dg) patients can be tracked through the Metabolic Clinic. UDOH is involved in a project within the Region looking at developing a registry system, data collection elements, and format at this time. UDOH does provide some services through the Metabolic Clinic for PKU and galactosemia (gg or Dg) only. Medical homes and families are notified of eligibility for this clinic upon diagnosis. 2) The state contacts the parents in addition to the physician. 3) State testing is sent out to a regional lab for newborn screening testing.

Appendix E. Business Practice Map by Scenario

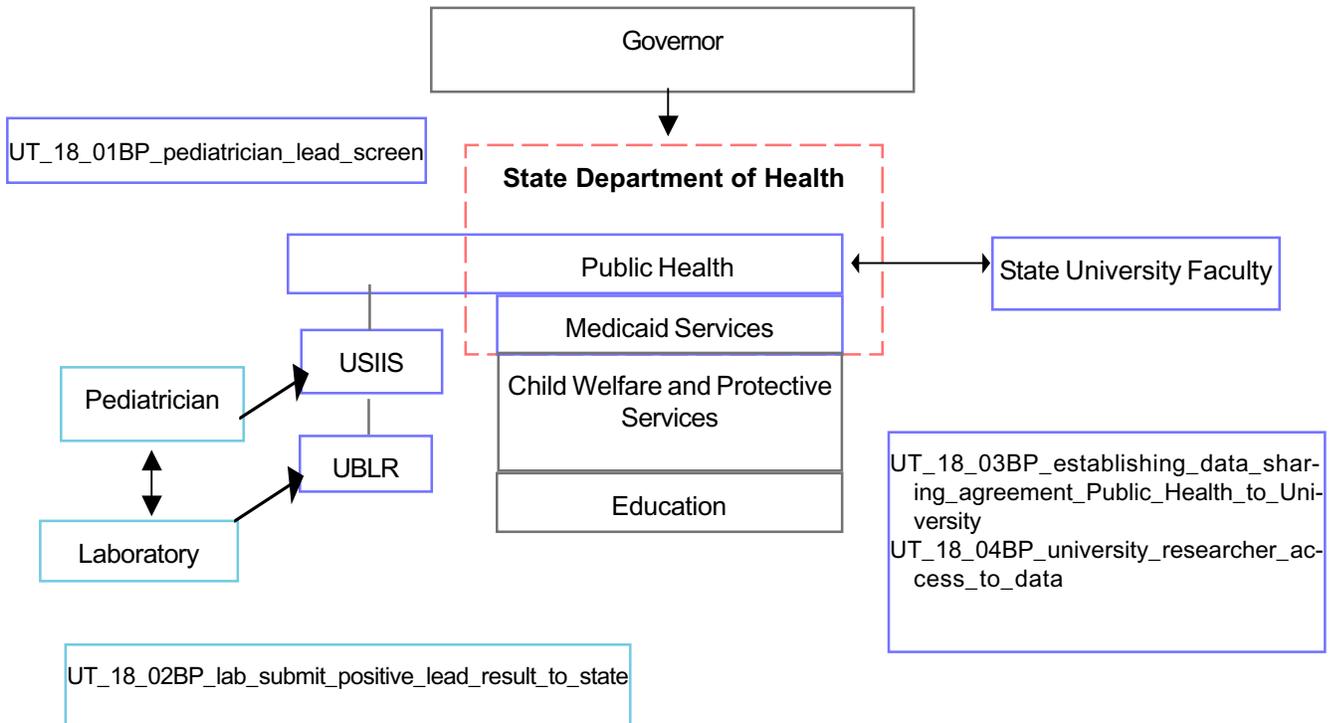
Public Health C



Observations: 1) As the primary care provider I feel this situation is not applicable. We do not have county shelters and we have no hospital-affiliated drug treatment clinics that serve the homeless. Our homeless are treated in social-based, not medical-based, facilities. 2) It is very rare that a homeless person would have a primary care provider. 3) The front end of this scenario did not apply to our state very well

Appendix E. Business Practice Map by Scenario

Government Oversight



Observations: The Department of Health maintains the Utah State Immunization Information Systems (USIIS) that holds records of children’s immunizations. Approximately 130 of 350 provider offices have enrolled with user confidentiality to have access to USIIS. All office staff of participating providers are granted access to USIIS. Access is renewed annually and any office staff that terminate employment or that are released are removed from having access. Only authorized health care users have access to USIIS. Utah also added lead poisoning to the injury surveillance and reporting system in 1990 per Utah Code R386 - 703 (Injury Reporting Rule).

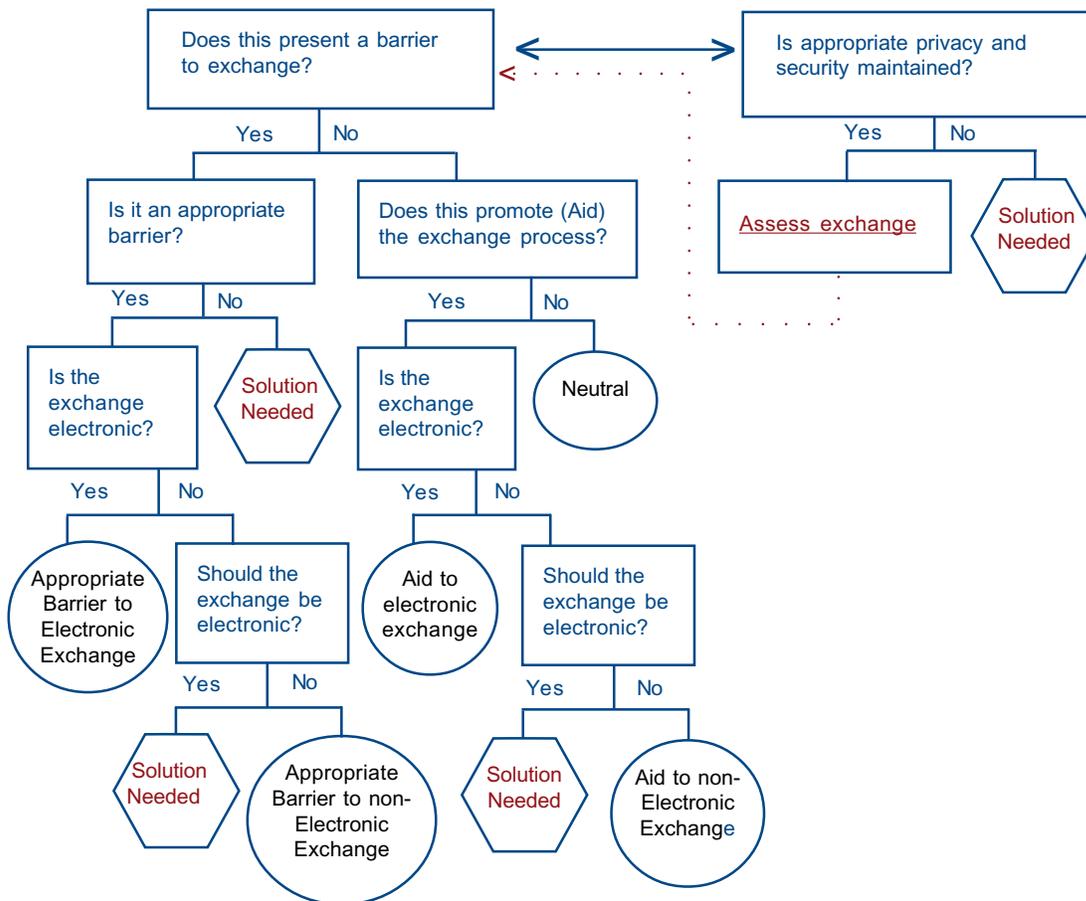
The state maps and tracks this information and it can easily be share with public officials. USIIS is widely used.

Appendix F. SWG Decision Tree

Appendix F. Solutions Work Group 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.

**Appendix G.
Legal Reference Guide
- Utah State Office of the At-
torney General¹¹**

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Citeⁱ

UCA 26-1-17.5(1)

Release of confidential records governed by this title

164.502 - Uses and Disclosures

Summary/Preemption Analysisⁱⁱ: Consistent / Analysis of this section is dependent on review of other section of this title. As is discussed in later sections of this analysis, it appears that UDOH covered entities can comply with both HIPAA and Title 26.

UCA 26-1-17.5(2)

Sharing immunization records with schools

164.512(b)(i) - Public Health Exception

Summary/Preemption Analysis: Consistent / HIPAA permits disclosure of PHI/IIHI by a covered entity for public health activities. Most sharing of immunization records will not be covered by HIPAA as this function in UDOH is performed by a non-covered entity.

UCA 26-1-30

Powers and duties of department

164.512(a) and (b)

Summary/Preemption Analysis: Consistent / Conduct of public health activities is supported by the HIPAA privacy rule.

UCA 26-2-3 to –28, except for –23 below

Vital Records

164.512(a) and (b); 160.203(c)

Summary/Preemption Analysis: Consistent / Collection of vital records is a core public health function required by law and consistent with HIPAA's requirements.

UCA 26-2-23

Records required to be kept by health care institutions – Information filed with local registrar and department

160.203(c), 164.512(a)

Summary/Preemption Analysis: Consistent / Hospitals are clearly covered entities under HIPAA. This statute requires hospitals to collect and report vital records. HIPAA authorizes release of PHI without patient consent for this type of public health activity. Covered entities can comply with this state law and HIPAA.

UCA 26-3-2

Voluntary collection of health data

164.512(b)

Summary/Preemption Analysis: Consistent / Section 512(b) of HIPAA authorizes covered entities to release data to public health authorities where the authority is authorized to receive the data. This voluntary reporting section authorizes the Department to receive a data report. It will protect covered entities that choose to voluntarily report.

UCA 26-3-4

Quality and publication of statistics as practicable

160.203

Summary/Preemption Analysis: Consistent / But for the qualification in this statute that publishing statistics only occur when it is practicable, HIPAA requirements may have been in conflict. If a UDOH covered entity determines that a statistical report has identifiable data, then the report would not be practicable.

ⁱ All references are found in 45 CFR. For example a listing of 160.203 refers to 45 CFR 160.203

ⁱⁱ *Consistent* indicates that the state statute does not appear to directly conflict with HIPAA. *Inconsistent* indicates that the state statute and the HIPAA rule appear to be in direct conflict. *Consistent in part* indicates that the state statute and the HIPAA rule appear to be consistent in part and inconsistent in part. Further analysis required indicates that a conclusion as to whether the state statute and HIPAA are consistent could not be reached and that further information and analysis is required. Beyond scope indicates that the state statute does not appear to intersect with HIPAA. For example, the statute may relate only to a non-covered entity (e.g., Department of Insurance).

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

UCA 26-3-6

Department may participate with other agencies to develop uniform standards for management of health information. 164.502

Summary/Preemption Analysis: Consistent / One of the primary goals of HIPAA was the standardization of health transactions between covered entities.

UCA 26-3-7(1)

Disclosure of health data – Consent required 164.502, 164.508, 164.502(g)

Summary/Preemption Analysis: Consistent in part / All of the 26-3-7 areas start with the premise that the Department may not release identifiable data unless allowed by one of the exceptions in this section. HIPAA requires that either the subject of the PHI or an appropriate representative consent to disclosure before releasing data, except for the 512 exceptions, such as public health. To the extent that these sections can be interpreted as consistent with HIPAA requirements, they will not be preempted.

- (a) the individual – this is consistent with HIPAA and will permit using a HIPAA compliant consent form.
- (b) the next-of-kin if the individual is deceased – HIPAA defers to state law on who is authorized to act on behalf of a deceased person. Under most circumstances next-of-kin are not authorized, absent court appointment to act on behalf of a deceased person. This section is not consistent with HIPAA and should not be followed by UDOH covered entities.
- (c) the parent or legal guardian if the individual is a minor or mentally incompetent – HIPAA defers to state law in this circumstance also. Unlike this statute, HIPAA distinguishes between emancipated and un-emancipated minors and makes it clear that a parent cannot authorize disclosure of a minor child's records if the child is authorized to make a treatment decision without the parents consent. In this latter circumstance, this section is not consistent with HIPAA and should not be followed by UDOH covered entities.
- (d) a person holding a power of attorney covering such matters on behalf of the individual – So long as the "covering such matters" language in this statute is interpreted to mean that the person has been granted authority to make health care decisions, then this section is consistent with HIPAA.

UCA 26-3-7(2)

Disclosure to another Government Entity. 164.512

Summary/Preemption Analysis: Consistent in part / This section is very much like a business associate agreement under HIPAA. The data must be used for the purpose for which it was collected. The government entity must agree not to further release the data and to safeguard the data. If the disclosure furthers a treatment, payment or operations activity of a covered entity, then the release would be allowed as a business associate relationship between the covered entity and the other government entity. If not, and the release is not permitted by one of the 512 exceptions, then for that circumstance this section would be inconsistent with HIPAA and should not be followed by a UDOH covered entity.

UCA 26-3-7(3)

Disclosure for Research or Statistical Purposes 164.512(i)

Summary/Preemption Analysis: Consistent / So long as UDOH rules continue to require an Institutional Review Board approval prior to allowing release of identifiable data for research, this section is consistent with HIPAA.

UCA 26-3-7(4)

Disclosure for Audit, Evaluation or Investigation of the Department 164.506(a), 164.512(a),(d)

Summary/Preemption Analysis: Consistent in part / Any release pursuant to this section that falls within the scope of treatment, payment or operations of the covered entity, may be accomplished pursuant to a business associate agreement and stay in compliance with HIPAA. Disclosures that are for health oversight

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

activities authorized by law are also permitted by HIPAA. Other releases in this area would not be consistent with HIPAA and should not be permitted by UDOH covered entities.

UCA 26-3-7(5)

Disclosure for Disease Surveillance 164.512(a),(b)

Summary/Preemption Analysis: Consistent / The releases discussed in this area are all within existing state law for disease surveillance or other authorized public health activities.

UCA 26-3-7(6)

Disclosure to Health Care Provider to Protect Patient or Others Closely Associated with the Patient
164.506(a)

Summary/Preemption Analysis: Consistent in part / UDOH covered entities may disclose PHI about a patient for the patient's own treatment under HIPAA. The language of this section authorizes a release, so the public health exception would validate any release within the scope of that exception. To the extent that any other contemplated release to protect others was required by law, HIPAA would also be consistent. Other releases would be inconsistent and should not be allowed by UDOH covered entities.

UCA 26-3-7(7)

Disclosures for Payment 164.506(a)

Summary/Preemption Analysis: Consistent / HIPAA allows releases for payment activities of covered entities.

UCA 26-3-7(8)

Disclosure to the Subject of the Identifiable Health Data
164.502

Summary/Preemption Analysis: Consistent / People generally have the right to access their own health data upon appropriate verification of identity under HIPAA.

UCA 26-3-8

Discretion of department to make disclosures under 26-3-7
164.502

Summary/Preemption Analysis: Consistent in part/ UDOH covered entities retain discretion on whether to permit a release of data in many circumstances. However, in the case of the right of the individual to access health data, UDOH covered entities would not have discretion and in this case this statute is inconsistent with HIPAA.

UCA 26-3-10

Department measures to protect security of health data
164.530(c)

Summary/Preemption Analysis: Consistent / The requirements of this section to safeguard identifiable health data mirror HIPAA requirements.

UCA 26-4-11, -14, -17, -23, -26, -27:

Medical Examiner Receipt and Release of Records 160.203(c), 164.512(a),(g),

Summary/Preemption Analysis: Consistent / The Medical Examiner is not a covered entity. Release and retention of records by the Medical Examiner is therefore not covered by HIPAA. The sections dealing with mandatory reporting to the Medical Examiner by covered entities is permissible under the 512 exceptions.

UCA 26-6-6:

Communicable Disease Reporting 164.5129(A)

Summary/Preemption Analysis: Consistent / Mandatory state reporting requirements, including communi-

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

cable diseases, is permitted under HIPAA.

UCA 26-6-18

VENEREAL DISEASE - CONSENT OF MINOR TO TREATMENT

164.502(g)(3).

Summary/Preemption Analysis: Consistent / HIPAA defers to state law regarding a minor's power under state law to make the medical decision. The CE may not notify parent without minor's consent.

UCA 26-6-27(1)

Information received by the Department regarding communicable or reportable disease confidential

160.203(c), 164.512

Summary/Preemption Analysis: Consistent / Communicable disease information is received and managed by entities within the UDOH that are not covered by HIPAA. If any local health department entity receiving data is part of a covered entity, the provisions in this section are not contrary to HIPAA and provide in some instances more protection of this data.

UCA 26-6-27(2)

Release of Communicable Disease Information

160.203(c), 164.512

Summary/Preemption Analysis: Consistent / Unlike UCA 26-3-7 which covers all data voluntarily supplied to the Department, this section is limited to communicable or reportable disease information. Most entities in state and local government dealing with this information will not be covered entities. However, even if they were covered entities, the broad public health and abuse reporting exceptions in HIPAA would permit this sharing of data.

UCA 26-6-29:

Violation for release of communicable or reportable disease information

160.203(c)

Summary/Preemption Analysis: Consistent / HIPAA permits state laws that are more protective to remain enforceable. Any covered entity can comply with both this section and HIPAA.

UCA 26-6-30

Exclusions from confidential requirements

164.512

Summary/Preemption Analysis: Consistent / This section merely says that the provisions of this chapter do not apply in certain circumstances. For covered entities, HIPAA would still apply in all circumstances, so there is no problem complying with this section.

UCA 26-6a-5

Reporting of possible communicable disease exposures to EMS personnel, reporting test results to patients

164.512(a),(b)(iv)

Summary/Preemption Analysis: Consistent in part / This mandatory public health reporting in this section is permissible under HIPAA. 26-6a-5(1)(d) mandates that a facility receiving a patient tested for AIDS or HIV infection withhold that information from a patient and allow Department personnel to provide those test results. The situations where HIPAA permits withholding information from a patient are quite limited and would not permit this blanket withholding of information. For covered entities, this section is preempted.

UCA 26-6a-7

Penalty for violation of confidential requirements'

160.203

Summary/Preemption Analysis: Consistent / States are free to be more protective of data.

UCA 26-6a-8

Appendix G. Legal Reference Guide

Utah Statute

HIPAA Cite

Patient notification and counseling

160.203

Consistent - Mandated counseling in this section does not violate any HIPAA provision.

UCA 26-6b-5 and -6

Quarantine, isolation and voluntary treatment

164.512

Consistent - Covered entities may comply with releasing information necessary to support public health interventions in this area due to the section 512 HIPAA exceptions.

UCA 26-8a-203

Emergency Medical Services Data collection

164.512

Summary/Preemption Analysis: Consistent / State laws that mandate reporting by covered entities are permitted by HIPAA.

UCA 26-8a-253

Statewide trauma registry and quality assurance program

164.512

Summary/Preemption Analysis: Consistent / State laws that mandate reporting by covered entities are permitted by HIPAA.

UCA 26-18-103

Drug Utilization Review Board – Responsibilities

164.506(a); 164.512(d)

Summary/Preemption Analysis: Consistent / The activities of the Drug Utilization Review Board are permitted as either a health oversight activity or as part of the treatment, payment or operations of government funded medical programs. Access to PHI by the board to conduct activities required by Utah law is permitted by HIPAA.

UCA 26-18-104

Confidentiality of records held by the DUR

164.508

Summary/Preemption Analysis: Consistent / The confidentiality requirements of this section are in harmony with HIPAA requirements.

UCA 26-19-18

Release of medical billing information regarding Medicaid recipient's restricted

164.502

Summary/Preemption Analysis: Inconsistent / This section seeks to restrict patient access to their own medical records to support third party liability collections undertaken on behalf of government funded medical programs. HIPAA does not permit this restriction and covered entities in Utah should not follow this section.

UCA 26-21-9

Application for license – Information required – Public records

160.202 (definition of “contrary”), 160.203, 164.512(a)

Summary/Preemption Analysis: Consistent / Licensing activities in the UDOH are not conducted by covered entities. The reporting required by this section is permitted by HIPAA under the 512(a) exception.

UCA 26-21-20

Mandate for Hospitals to Provide Itemized List of Charges

164.502

Summary/Preemption Analysis: Consistent in part / Two areas of this law are not consistent with HIPAA. The overall requirement to provide an itemized list of charges at the hospital's expense is permissible, except in the case of an “agent”. This term is not defined and could be inconsistent with HIPAA's requirement of limiting access to the patient or someone authorized to make health care decisions on behalf of the

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

patient. Section (5), like 26-19-18 limits access by Medicaid recipients to their own medical records. This restriction is inconsistent with HIPAA and should not be followed by covered entities.

UCA 26-23a-2

Injury reporting requirements

164.512(a)

Summary/Preemption Analysis: Consistent / State laws that mandate reporting by covered entities are permitted by HIPAA.

UCA 26-23b-103

Detection of Public Health Emergencies - Mandatory reporting requirements

164.512(a)

Summary/Preemption Analysis: Consistent / State laws that mandate reporting by covered entities are permitted by HIPAA.

UCA 26-23b-104

Public Health Emergencies: Authorization to report

160.203(c), 164.512(b)

Summary/Preemption Analysis: Consistent / This section authorizes reporting of medical observations by certain providers that suspect an epidemic disease or bio-terrorism event may be involved. The public health exception in 164.512(b) expressly recognizes authorized, but not required, reporting as valid under HIPAA. This section becomes mandatory in the event a public health emergency is declared.

UCA 26-23b-108

Investigation of suspected bioterrorism and communicable diseases-requirement to destroy records

160.203(c), 164.512(a), 164.512(j)

Summary/Preemption Analysis: Consistent in part / For all UDOH activities this section is valid, since none of the entities involved in this activity are covered by HIPAA. If a local health department engaged in this activity is part of a covered entity, then the covered entity may need to retain the records consistent with the entities policy for retention of records regarding treatment of a patient.

UCA 26-25-1 to -5

Health Oversight Reporting

160.203(c), 164.512(d)

Summary/Preemption Analysis: Consistent in part / Health oversight activities authorized by law may receive data from covered entities without the patient's permission under 164.512(d). Subsection (3) makes it clear that the purpose of the releases authorized by this state law is improvement of health care. Most entities receiving data under this would not be covered entities. If a covered entity receives data under this section, and includes that data in the facility's designated record set, access to identifiable data would be governed by HIPAA requirements and the provisions of this section that would deny access under circumstances where HIPAA permits access would be preempted

UCA 26-33a-104, -106, -108, -109, -111

Health Data Committee - purpose, powers and duties of the committee

164.512(a)

Summary/Preemption Analysis: Consistent / State laws that mandate reporting by covered entities are permitted by HIPAA.

UCA 26-45-103, -104

Genetic Privacy Act -Restrictions on employers and insurers 160.203

Summary/Preemption Analysis: Consistent / State laws that afford additional protection to a patient's expectation of health information privacy are permitted under HIPAA so long as a patient's access is not unduly restricted. This law provides greater protection for a patient's PHI, in that it prohibits disclosures of

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

the genetic test results to employers or health plans (except in very restricted circumstances), as well as imposes minimum necessary restrictions on PHI release to health plans for payment purposes. This law does not allow the CE to honor an authorization signed by the patient to release genetic tests results to the employer or health plan. This does not cause a preemption issue because the privacy regulations do not compel the CE to honor an authorization by the patient.

UCA 26A-1-114: Powers and duties of local health departments 164.512

Summary/Preemption Analysis: Consistent / State laws that mandate reporting by covered entities are permitted by HIPAA. In addition public health activities are seen as a national priority and HIPAA is intended to not interfere with traditional public health activities.

UCA 30-2-9

Family Expenses

164.522(a)

Summary/Preemption Analysis: Consistent / CE may disclose information to patient's spouse if spouse is involved in paying medical bills. HIPAA does not prohibit a disclosure to a spouse if the CE needs to disclose it for its own payment activities, unless the patient has requested a restriction to the disclosure, and the CE agreed. 67 Fed. Reg. 53182,53203

UCA 31A-31-101 to -108

Insurance Fraud Act - Reports to Government Agencies and Insurers

164.512(d), 164.506(c)

Summary/Preemption Analysis: Consistent / This act authorizes health care providers to share information about insurance fraud with various government agencies, including the Department of Insurance and the Attorney General's Office. The Health Oversight reporting provisions of HIPAA at 164.512(d) permit this. Reports to insurers are also permitted by HIPAA as operations when both parties have a relationship with the patient.

UCA 53-3-303(14)(c)

Reporting impaired driver

164.512

Summary/Preemption Analysis: Consistent in part / A health care professional is granted immunity for a good faith report on an impaired driver. Nothing in this section requires reporting. If the report is authorized by one of the section 512 exceptions, such as to avoid an imminent danger and the report is made to someone that can intervene, then this section is not impacted. In all other circumstances, the CE should obtain patient consent before making the report.

UCA 58-13-5(3)(h)

Mandatory Report to Division of Occupational and Professional Licensing of health care provider abusing alcohol or drugs

165.512

Summary/Preemption Analysis: Consistent / State laws that mandate reporting by covered entities are permitted by HIPAA. Covered entities should be aware that HIPAA does not preempt the stricter standards imposed by 42 CFR Part 2 (Confidentiality of Alcohol and Drug Abuse Patient Records) for any provider participating in a treatment program covered by that section. Analysis of whether 42 CFR Part 2 preempts this section of state law is beyond the scope of this analysis.

UCA 62A-3-206

Long-term Care Ombudsman

164.512(d) 160.203(b)

Summary/Preemption Analysis: Consistent / This Utah law is not contrary to HIPAA; a covered entity may comply with both. According to the DHHS Administration on Aging (see AOA-IM-03-01) the LTCOP is a "health oversight agency" and the Privacy Rule does not preclude release of residents' clinical records to the LTCOP with or without authorization of the resident or residents' legal representative. The UCA provision

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

regarding written permission is more protective of an individual's privacy than HIPAA.

UCA 62A-3-207

LTCOP files are confidential, disclosure at ombudsman's discretion.
160.102

Summary/Preemption Analysis: Consistent / The LTCOP is not a covered entity, therefore HIPAA does not preempt its use/disclosure of health information. GRAMA applies.

UCA 62A-3-303

Adult Protective Services access to facilities and records 164.512(c), 160.203(c)

Summary/Preemption Analysis: Consistent / HIPAA defers to state law regarding reporting abuse or neglect, and a covered entity may comply with both. A covered entity may disclose PHI about a suspected victim of abuse or neglect to a protective services agency to the extent the disclosure is required by law, and the disclosure complies with and is limited to the requirements of such law. The covered entity is required to inform the individual that the report is being made unless the covered entity believes informing the individual will place the individual at risk of serious harm, or unless they'd be informing the individual's personal representative, they believe the PR is responsible for the neglect or abuse, and informing the PR would not be in the individual's best interest.

UCA 62A-3-304

Caretaker, facility or institution may not use its confidentiality standards as a basis for failure to report to APS 164.512(c), 160.203(c)

Summary/Preemption Analysis: Consistent / HIPAA defers to state law regarding reporting abuse or neglect, and a covered entity may comply with both. A covered entity may disclose PHI about a suspected victim of abuse or neglect to a protective services agency to the extent the disclosure is required by, complies with and is limited to the requirements of law.

UCA 62A-3-305

requires persons to notify Adult Protective Services intake or the nearest law enforcement agency of abuse / neglect. 164.512(a)(1) 164.512(c) 160.203(c)

Summary/Preemption Analysis: Consistent / HIPAA defers to state law regarding reporting abuse or neglect, and a covered entity may comply with both. A covered entity may disclose PHI about a suspected victim of abuse or neglect to a protective services agency to the extent the disclosure is required by law, and the disclosure complies with and is limited to the requirements of such law. The covered entity is required to inform the individual that the report is being made unless the covered entity believes informing the individual will place the individual at risk of serious harm, or unless they'd be informing the individual's personal representative, they believe the PR is responsible for the neglect or abuse, and informing the PR would not be in the individual's best interest.

UCA 62A-3-311.1

The Division of Aging and Adult Services maintains a data base for reports of vulnerable adult abuse / neglect for specified purposes 160.102

Summary/Preemption Analysis: Consistent / The Division of Aging and Adult Services is not a covered entity, therefore HIPAA does not preempt its use/disclosure of health information. GRAMA applies.

UCA 62A-3-312

The DAAS data base and case files are classified as protected under GRAMA; disclosures are limited to specified individuals. 160.102

Summary/Preemption Analysis: Consistent / The Division of Aging and Adult Services is not a covered entity, therefore HIPAA does not preempt its use/disclosure of health information. GRAMA applies.

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

UCA 62A-4a-116

The Division of Child and Family Services maintains protected records in a Management Information System; disclosures are limited to specified individuals. 160.102

Summary/Preemption Analysis: Consistent / The Division of Child and Family Services is not a covered entity, therefore HIPAA does not preempt its use/disclosure of health information. GRAMA applies.

62A-4a-116.1 and 116.2

DCFS maintains protected records in a Licensing Information System; disclosures are limited to specified individuals. 160.102

Summary/Preemption Analysis: Consistent / The Division of Child and Family Services and the Office of Licensing are not covered entities, therefore HIPAA does not preempt their use/disclosure of health information. GRAMA applies.

UCA 62A-4a-116.5

DCFS sends a notice to a person with respect to whom it makes a finding of abuse/neglect/dependency, and the person has the right to request a copy of the report.

160.102

Summary/Preemption Analysis: Consistent / The Division of Child and Family Services is not a covered entity, therefore HIPAA does not preempt its use/disclosure of health information. GRAMA applies.

62A-4a-202.3

When DCFS takes a child into protective custody, the investigation includes a review of any reports of past abuse/neglect involving the child, siblings, and other children in the household, interviews of health care providers, and a medical examination of the child. 164.512(b) 160.203(c)

Summary/Preemption Analysis: Consistent / UCA §62A-4a-202.3 is not preempted by HIPAA. A covered entity may disclose PHI to appropriate governmental authority authorized by law to receive reports of child abuse or neglect. HIPAA permits a covered entity to comply with both UCA and HIPAA.

62A-4a-205

An interdisciplinary team, including a mental health representative, creates a treatment plan that provides for the health, safety and welfare of a child in temporary DCFS custody, including the health and mental health care to be provided to the child. The plan is provided to the GAL, natural and foster parents.

160.102

Summary/Preemption Analysis: Consistent / DCFS is not a covered entity, therefore HIPAA does not preempt its use/disclosure of health information. GRAMA applies. The mental health representative may or may not be part of a covered entity. Even if covered, the mental health representative may help create a treatment plan without wrongfully using or disclosing PHI.

62A-4a-403

Requires persons to notify DCFS or the nearest law enforcement agency of abuse / neglect.

164.512(a)(1) 164.512(b) 160.203(c)

Summary/Preemption Analysis: Consistent / 62A-4a-403 is not preempted by HIPAA. A covered entity may disclose PHI to appropriate governmental authority authorized by law to receive reports of child abuse or neglect. HIPAA permits a covered entity to comply with both UCA and HIPAA.

62A-4a-404

Requires persons to notify DCFS at the time of birth when the child has fetal alcohol syndrome or fetal drug dependency

164.512(a)(1),(b) 160.203(c)

Summary/Preemption Analysis: Consistent / A covered entity may disclose PHI to appropriate govern-

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

mental authority authorized by law to receive reports of child abuse or neglect, and disclosures required by law that comply with and are limited to the requirements of such law. HIPAA permits a covered entity to comply with both UCA and HIPAA.

62A-4a-405

Requires persons who believe a child died from abuse/neglect to notify law enforcement. The medical examiner shall disclose his report to specified persons. 164.512(a)(1),(b) 160.203(c)

Summary/Preemption Analysis: Consistent / A covered entity may disclose PHI to appropriate governmental authority authorized by law to receive reports of child abuse or neglect, and disclosures required by law that comply with and are limited to the requirements of such law. HIPAA permits a covered entity to comply with both UCA and HIPAA.

62A-4a-406

Permits photos to be taken of child's injuries and authorizes all medical records pertinent to an investigation to be disclosed to DCFS & law enforcement. 164.512(b) 160.203(c)

Summary/Preemption Analysis: Consistent / A covered entity may disclose PHI to appropriate governmental authority authorized by law to receive reports of child abuse or neglect. HIPAA permits a covered entity to comply with both UCA and HIPAA.

62A-4a-407

Permits a physician examining a child, who believes the child's life/safety is in danger, to take the child into protective custody and notify DCFS. 164.512(b); 160.203(c)

Summary/Preemption Analysis: Consistent / A covered entity may disclose PHI to appropriate governmental authority authorized by law to receive reports of child abuse or neglect. HIPAA permits a covered entity to comply with both UCA and HIPAA.

UCA 62A-4a-409

DCFS pre-removal investigation shall use an interdisciplinary team whenever possible, including health and mental health representatives, to assist with diagnostic, treatment, and coordination services.

160.102 164.512(a)(1)

Summary/Preemption Analysis: Consistent / DCFS is not a covered entity, therefore HIPAA does not preempt its use/disclosure of health information. GRAMA applies. Health or mental health representatives may use or disclose PHI to assist with diagnostic, treatment, and coordination services, as required by 62A-4a-409.

UCA 62A-4a-801 to -802

Safe Relinquishment of a Newborn Child

164.504, 164.512

Summary/Preemption Analysis: Consistent / Hospitals are authorized to receive a newborn child from a parent or the parent's designee. Hospitals are required to render appropriate care and transfer the child to the Division of Child and Family Services. Hospitals will receive medical information either from the parent or in the course of treating the child. If the hospital gathers information that suggests abuse or neglect, law requires reporting this information to DCFS. The same applies to reports to Vital Records.

UCA 62A-7-121

Youth offender records are the property of the Division of Youth Corrections and shall be returned to it when the youth offender is terminated from the program. 164.512, 164.524

Summary/Preemption Analysis: Consistent in part / This law will require covered entities under contract with the Division of Youth Corrections to release all records to the Division as required by law. This statute, if applied by the DYC to require covered entities to turn over original treatment records and not to retain any copies, would deny patient access to records as required by 164.524. It would also inhibit the ability of a

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

covered entity to assist in the treatment of a patients who either returns for additional treatment or seeks to have records sent to a new provider that needs information about past treatment activity. It would further leave the covered entity unable to defend itself against claims of malpractice. In this situation. HIPAA would preempt this section of state law.

UCA 63-2-107

[Governmental Records Act does not apply to government entities covered by HIPAA.](#)
Parts 160 and 164

Summary/Preemption Analysis: Consistent / The workgroup identified GRAMA as having preemption problems in the fall of 2002. This section of law was adopted during the 2003 Legislative session. Government covered entities follow HIPAA.

UCA 63-25a-416 to -418

[Crime Victim's Reparation- Applicant waiver of privilege and requirement to supply medical or psychological reports](#)
164.524

Summary/Preemption Analysis: Beyond Scope / The Crime Victims' Reparations Board is not a covered entity under HIPAA. If an applicant fails to submit to tests or to supply necessary information, the only remedy is to deny the claim. This section implicates no covered entity's duties under HIPAA.

UCA 64-13-27(1)

[Department of Corrections centralized record of offenders](#) 160.103

Summary/Preemption Analysis: Beyond Scope / This centralized record will contain health records about individuals. The Department of Corrections is not a covered entity, thus this section is beyond the scope of HIPAA.

UCA 64-13-27(2)

[Department of Corrections Records are the property of the Department.](#)
164.512, 164.524

Summary/Preemption Analysis: Consistent in part / This law will require covered entities under contract with the Department of Corrections to release all records to the Department as required by law. This statute, if applied by the DOC to require covered entities to turn over original treatment records and not to retain any copies, would deny patient access to records as required by 164.524. It would also inhibit the ability of a covered entity to assist in the treatment of a patients who either returns for additional treatment or seeks to have records sent to a new provider that needs information about past treatment activity. It would further leave the covered entity unable to defend itself against claims of malpractice. In this situation. HIPAA would preempt this section of state law.

UCA 64-13-36

[Department of Corrections Testing of prisoners for AIDS and HIV Infection](#)
160.103

Summary/Preemption Analysis: Beyond Scope / This centralized record will contain health records about individuals. The Department of Corrections is not a covered entity, thus this section is beyond the scope of HIPAA.

UCA 67-4a-301

[Report of Abandoned Property to Deputy State Treasurer](#) 164.512(a)

Summary/Preemption Analysis: Consistent / Covered entities may hold abandoned property subject to this act and be required to report PHI in response to the requirements of this law. State laws that mandate reporting by covered entities are permitted by HIPAA.

UCA 67-4a-701

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

Treasurer May Examine Records to Verify Compliance **164.512**

Summary/Preemption Analysis: Consistent / HIPAA also permits the examination of records pursuant to section 512(a) to the extent required by law.

UCA 76-5-504

Notification of HIV and AIDS status of offender to victim 164.512

Summary/Preemption Analysis: Consistent / State laws that mandate reporting by covered entities are permitted by HIPAA. To the extent that local health departments conduct this activity through a covered entity, release of information to a victim would be permitted without the patient's consent.

UCA 76-7-304(2)

Informing parent or spouse prior to abortion 164.502(g)(3)

Summary/Preemption Analysis: Further Analysis Required / A doctor performing an abortion to a minor must notify the parent, if possible. Under UCA 78-14-5(4)(f) any female has power to consent where pregnancy or childbirth is involved. Further analysis of the interaction of this state law and HIPAA is required.

UCA 76-7-325

Informing Parent or Spouse Prior to Providing Contraceptives.
164.502(g)(3)

Summary/Preemption Analysis: Further Analysis Required / Any person providing contraceptives to a minor must notify the parent, if possible. Under UCA 78-14-5(4)(f) any female has power to consent where pregnancy or childbirth is involved. Further analysis of the interaction of this state law and HIPAA is required..

UCA 78-14-5(4)(f)

CONSENT INVOLVING PREGNANCY OR CHILDBIRTH 164.502(g)(3)

Summary/Preemption Analysis: Further Analysis Required / HIPAA defers to state law regarding a parent's access to the records of an unemancipated minor. Further analysis is needed to determine whether a CE may notify the parent without the minor's consent.

UCA 78-25-25

Patient Access to Medical Records 164.524

Summary/Preemption Analysis: Consistent / The workgroup identified this section as having preemption problems in the fall of 2002. The old section of this law was repealed and the current language substituted during the 2003 Legislative session. All health care providers, regardless of whether they are covered by HIPAA must grant access to patients and their personal representatives, absent a judicial or other restriction authorized by law. Providers may charge a reasonable copying fee.

Administrative Rules

Summary / Preemption Analysis

R612-2-3

Worker's Compensation Rules- Health Care Providers- filing initial examination of industrial patient's injury, follow up disclosures of SOAP or progress notes, return to work forms

164.512(6)(l)

Summary/Preemption Analysis: Consistent / Privacy regulation allows for disclosures for workers' compensation or other similar programs, established by law

R612-2-22

Appendix G. Legal Reference Guide
Utah Statute

HIPAA Cite

[Access to medical records, charging for copies and obtaining copies of medical records in industrial cases](#)
160.203

Summary/Preemption Analysis: Beyond Scope / The Industrial Commission is not a covered entity, thus this section is beyond the scope of HIPAA. Amendments adopted in July 2003, grant very broad access pursuant to this rule. The agency and the Administrative Rules Review Committee are examining changes to this section. Some have suggested that the fee schedule set by this rule could be a benchmark for covered entities on what is a reasonable charge. The Workgroup took no position on this suggestion.

REFERENCES

- ¹ Privacy and Security Solutions for Interoperable Health Information Exchange National Conference (n.d.) Retrieved February 15, 2007 from http://healthit.ahrq.gov/portal/server.pt?open=514&objID=5562&mode=2&holderDisplayURL=http://prodportallb.ahrq.gov:7087/publishedcontent/publish/communities/a_e/ahrq_funded_projects/rti_public_page/main.html Foundation of Research and Education of American Health Information Management Association. Development of State Level Health Information Exchange Initiatives: Final Report. September 1, 2000
- ² Foundation of Research and Education of American Health Information Management Association. Development of State Level Health Information Exchange Initiatives: Final Report. September 1, 2006
- ³ The Utah Digital Health Service Commission is an eleven member public-private commission appointed by the governor. See Utah code 26-9f-104.
- ⁴ Broderick, M., Smaltz, D. H. (2003, May). HIMSS SIG White Paper. Retrieved February 18, 2007 www.himss.org/content/files/ehealth_whitepaper.pdf
- ⁵ UDOH Receives Grant to Improve the Exchange of Electronic Health Information (2006, 5) Retrieved February 15, 2007 from <http://health.utah.gov/uthealthnews/20060524-HealthInfoGrant.htm>
- ⁶ Utah Department of Health Executive Director to Serve on State Alliance for e-Healthy (2007, 1) <http://health.utah.gov/uthealthnews/2007/20070111-eHealth.htm>
- ⁷ HealthInsight is participating in several other health information technology projects and was a founder of, and serves on, the Board of the Utah Health Information Network (UHIN). UHIN was the recipient of one of five grants provided by AHRQ in 2004 to begin establishing regional health information networks. The principal investigator on that grant was Scott Williams, MD (replaced as PI by UHIN assistant to the executive director Jan Root) who also served as the VP, Medical Affairs for HealthInsight (now Dr. Kim Bateman). HealthInsight is also responsible for the evaluation of that grant and is leading a subgroup to involve practicing physicians while having hosted a stakeholder conference to discuss the effect of HIT on quality and cost. HealthInsight has been partnering with the University of Utah for several years on a project to create Web and PDA-based decision support software for use by rural physicians. The CDC and AHRQ have provided funding for this project. The technology has been adopted by physicians in Utah, Idaho and Nevada and has successfully decreased the use of unnecessary antibiotics in those communities where it has been tested. Under funding from AHRQ, HealthInsight has also been working with the University of Utah primary care clinics to increase the use of certain preventive tests through the use of decision support tools designed specifically for their current EMR. The pilot has been successful and the University and HealthInsight are seeking additional funding to expand the program to independent clinics in Utah.
- ⁸ John Nelson, MD served as the 159th President of the American Medical Association (AMA) from June 2004 to June 2005. A recognized and influential leader in Utah's public health activities, Dr. Nelson is a former deputy director of Utah's Department of Health and has served on the governor's task forces on child abuse and neglect and teenage pregnancy prevention. A board-certified ob-gyn, Dr. Nelson has a private ob-gyn practice in Salt Lake City. He is a diplomat of the American Board of Obstetrics and Gynecology and a fellow of the American College of Obstetricians and Gynecologists.
- ⁹ Lyle Odendahl, JD has represented UDOH at administrative hearings and served as administrative law judge. He has advised UDOH programs on requirements for compliance with the HIPAA Privacy and Security rules; has experience working with health industry groups to build coalitions and to negotiate draft legislation and served as legal advisor to the Health Policy Commission to develop and draft health care reform legislation. In addition he was a gubernatorial appointment to the Information Practices Act Task Force that developed the Utah Government Records Access Management Act (GRAMA) and lectured on records privacy issues before the National Association of Government Archives and Records Administrators.
- ¹⁰ 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>.
- ¹¹ HIPAA Preemption Analysis. Utah State Office of the Attorney General. November 17, 2003.