

Interoperable Solutions for Health Information Exchange:

A survey of health information exchange practices in
Utah.



November 2006

Submitted by:

Lois Haggard, Ph.D., Project Director
Utah Department of Health
PO Box 142101
Salt Lake City, UT 84111-2101

Submitted to:

Cynthia Irvin, Ph.D., State Liaison
Privacy and Security Solutions for Interoperable Health Information Exchange
Research Triangle Institute
PO Box 12194
3040 Cornwallis Road
Research Triangle Park, NC
Contract No. 290-05-0015

November 2006

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

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

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. These participants' voluntary time and input has been critical in identifying and documenting the privacy and security concerns in health information exchange.

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

CONTENTS

Executive Summary	1
<i>Summary Findings</i>	
<i>Background</i>	
<i>Stakeholder Relations</i>	
<i>e-Health in Utah</i>	
Methodology	4
<i>Overview</i>	
<i>Variation Work Group</i>	
<i>Legal Work Group</i>	
<i>Data Collection</i>	
Findings - Treatment Setting	6
<i>Scenario Review (1-4)</i>	
<i>Stakeholders - Treatment</i>	
<i>Variation - Treatment</i>	
<i>Critical Observations</i>	
Findings - Payment	11
<i>Scenario Review (5)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - RHIO	13
<i>Scenario Review (6)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - Research Data Use	14
<i>Scenario Review (7)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - Access by Law Enforcement	16
<i>Scenario Review (8)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - Prescription Drug Use/Benefit	18
<i>Scenario Review (9&10)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - Healthcare Operations & Marketing	20
<i>Scenario Review (11 & 12)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - Bioterrorism Event	22
<i>Scenario Review (13)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - Employee Health	24
<i>Scenario Review (14)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - Public Health (A, B & C)	25
<i>Scenario Review (15-17)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Findings - Health Oversight/Government Compliance	29
<i>Scenario Review (18)</i>	
<i>Stakeholders</i>	
<i>Variation</i>	
<i>Critical Observations</i>	
Conclusion	30
Notes	31

EXECUTIVE SUMMARY

Achieving an interoperable system of health information exchange (HIE) leaves much to consider in terms of individuals' privacy and the security of their health information. The reality of an interoperable system that preserves the public's confidence in the privacy of their information remains a huge challenge for the health care industry. Add to that exchanges among entities that are governed according to different regulations, for example: law enforcement, state labs, drug treatment facilities or public health, and the challenges magnify. As Utah moves e-Health forward, it becomes critical to define with whom, and under what conditions, HIE interoperability is achieved.

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 Commission¹, is engaging stakeholders in healthcare, law enforcement, public health, consumers and other arenas in a discussion to examine privacy and security issues related to HIE. Phase one of this project has been to assess the degree to which variation exists among stakeholder business practices regarding the exchange of health information. The Research Triangle Institute (RTI) provided eighteen scenarios covering various types of health information exchanges and business partners and organizations involved in the exchanges. The scenarios were designed to promote discussion of privacy and security practices. Phase two will identify solutions to identified barriers to HIE uncovered during phase one. Phase three involves the development of a plan to implement the solutions.

This report documents variation among organizational-level practices and procedures for the exchange of patient health information depicted in the scenarios. The information contained in this report was gathered through a series of meetings, surveys, and interviews with stakeholders in the project work groups and the broader Utah stakeholder community. Business practice data were collected using the RTI scenarios.

This report represents a synthesis of information and discussions from meetings of the Variations and Legal Work Groups. The document contains the following:

- Summary findings for each of the ten RTI scenario-based purposes of health informa-

tion exchange.

- RTI scenarios.
- A brief description of the Stakeholders that responded to the scenarios.
- Critical observations and legal analysis.

Summary Findings

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

Transmission and transmission security of Protected Health Information (PHI). There is substantial variation in the means of transmission and security employed. On one hand, we have physicians (in a physician office setting) who reported regularly disclosing health information over the phone to other health care professionals as long as there was a common level of understanding and trust. On the other extreme, substance abuse providers have developed complex procedures for transmission that include: verification, physical safeguards, warnings on paperwork about 42 CFR Part 2, and required acknowledgment receipts.

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

Electronic methods (CDs and the Internet) reportedly

are employed with radiology films (e.g. x-rays), especially among large facilities. Mammography films are a unique case in Utah. Some selected large facilities having the capability to make CD's and use the Internet (by Picture Archiving and Communication System - PACS) to transfer mammography films, but they reported rarely using these methods. Instead, films are typically transferred by in-person pick-up with approved photo identification or sent by U.S. mail.

Applicability of relevant rules and statutes. Difficulty in exchanging health information increases when different rules and statutes apply to entities involved in the exchange of health information. Law enforcement is not a covered entity under HIPAA nor are Public Health or State Public Health Laboratories. Although substance treatment facilities are covered entities, they must also comply with 42 CFR Part 2, a federal regulation that heightens protections for treatment records. Primary care providers may disregard treatment facilities' records because of the associated difficulties. HIPAA and 42 CFR Part 2 do not align in a manner that is conducive to health information exchange.

The privacy and security concerns identified in this report are a mix of organizational, technological, educational, and legal issues. This is likely due to the nature of the scenarios used to collect the business practice data. Some scenarios illustrated atypical events that require the exchange of health information with agencies outside of the healthcare arena (e.g. law enforcement).

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 e-Health 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.

Background

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 computer-

ized 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 long been a leader in biomedical informatics research, since the founding of the Department of Medical Informatics in 1972 at the University of Utah.

In 2004 Utah Health Information Network (UHIN) was awarded a multi-year contract from the Agency for Healthcare Research and Quality (AHRQ) to function as a Regional Health Information Organization (RHIO). UHIN's five-year strategic plan includes developing exchanges of clinical information. Specific planned clinical data sharing projects include laboratory results, chief complaint, chart notes, hospital discharge notes, continuity of care records, and e-prescribing. Workgroups comprised of volunteers from the community of stakeholders interested in these exchanges are actively working to develop the standards that will serve as the basis for these exchanges.

The Utah Department of Health obtained funding in December, 2005 from the Robert Wood Johnson Foundation InformationLinks Project for the UNIFY initiative, the Utah Network for Electronic Public Health Information. UNIFY has begun a yearlong planning effort to develop a business plan for Public Health participation in clinical exchanges. UNIFY has the goal of evaluating the business case for all the potentially valuable exchanges between the clinical care sector and Public Health, but is especially focused on surveillance of reportable diseases, vital records, newborn screening and immunizations. 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 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.

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.

Stakeholder Relations

Utah 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 wisely opted to stay within the American National Standards Institute (ANSI) X12 framework and, indeed, 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.

E-Health In Utah

A measure of the maturity of HIT initiatives in Utah is that our focus is 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 our 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.

METHODOLOGY

Overview

UNIFY-PS for the Utah Network for Electronic Public Health Information, Privacy and Security is part of the national collaborative project. All 33 participating states and Puerto Rico adhere to a similar work plan established by the Agency for Healthcare Research and Quality (AHRQ) and RTI. The work is accomplished through volunteer workgroups. Community input was assured through membership in each workgroup.

The work plan involves five workgroups, as follows:

Variations Workgroup. Sponsored by HealthInsight, this group conducted a broad canvass 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 present barriers to exchange of information.

Legal Workgroup. Sponsored by the Utah Attorney General's Office, this group reviewed the business practices and policies identified by the Variations Workgroup, and identified the relevant law driving associated practices where applicable.

Solutions Workgroup. Sponsored by the Utah Health Information Network (UHIN), this group will examine any problematic variations and propose solutions for Utah, and respond to national solutions generated by AHRQ and RTI. They will seek solutions that are legal and ethical, and feasible in Utah's healthcare and public health contexts.

Implementation Workgroup. Sponsored by the Utah Department of Health, this group will explore implementation strategies for the identified privacy and security solutions.

Steering Committee. This group, consisting of all four workgroup chairs and the members of Utah Digital Health Services Commission, provides project oversight and reviews the work processes and work products of each of the other four workgroups.

Variations Work Group

John Nelson, MD, chairs the Variations Work Group (VWG)². Dr. Nelson is an obstetrician-gynecologist from Salt Lake City, and a Medical Director at HealthInsight³, Utah. HealthInsight is a private, nonprofit quality improvement organization (QIO) whose mission is to be a catalyst in the transformation and improvement of the health care system. In their thirty-year history, HealthInsight has worked with the health care community on initiatives to improve the quality of care delivered in Nevada and Utah. In doing so, they have become a trusted and neutral facilitator of health care improvement.

HealthInsight works with hospitals, physician clinics, home health agencies, long-term care facilities, health plans, and legislative and government agencies. One of four QIOs chosen in 2004 by Centers for Medicare & Medicaid Services (CMS) to pilot the national Doctors' Office Quality Information Technology (DOQ-IT) project which promotes the adoption of electronic health record (EHR) systems and information technology (IT) in small-to-medium sized physician offices with a vision of enhancing access to patient information, decision support, and reference data, as well as improving patient-clinician communications.

The DOQ-IT program at HealthInsight is currently working directly with over 200 primary care clinics in Utah (over 60% of the total primary care clinics in Utah.) Approximately 40% of the participating clinics are in rural communities. Over half of the clinics now have an EMR and are continuing to progress through the stages of implementation toward full decision support.

HealthInsight has ongoing statewide connection with health providers and payers, especially familiar with rural health care providers. HealthInsight is the lead organization charged with overseeing the work of the Variations Workgroup. The workgroup committee is a fourteen-member committee comprised of stakeholders representing physicians, pharmacists, hospitals, law enforcement, payers, RHIO, consumers, long-term care facilities, public health, laboratories, and state agencies. See Appendix A.

Legal Work Group

Lyle Odendahl, JD⁴, an Assistant Attorney General for the state of Utah chairs the Legal Work Group (LWG). He provides advice to policymakers and staff of the Utah

Department of Health (UDOH). The mission of the Office of the Utah Attorney General is to uphold the constitutions of the United States and of Utah, enforce the law, provide counsel to state agencies and public officials, assist law enforcement, and protect the interests of the state, its people, environment and resources.

The Utah Attorney General's Office assigns five Assistant Attorney Generals to provide the legal consultation to the entire UDOH. Mr. Odendahl and four other attorneys representing public, private and consumer stakeholder interests provide legal consultation and direction to the project. See Appendix B.

Data Collection

The VWG was tasked with collecting and assessing variations in organization-level business policies and practices and categorizing them as barriers or non-barriers with respect to interoperability. The LWG was tasked with assessing applicable privacy and security policies, underlying statutes, regulations, court cases, etc. and identifying legal sources of barriers to interoperability. In addition, the LWG reviewed the barriers uncovered in the business practice assessment and mapping, and identified applicable state and federal privacy and security laws.

The ad hoc VWG began to recruit stakeholders based on guidance outlined in the original proposal. Release of the scenarios indicated that additional stakeholders were needed to collect 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. Efforts were made to create a representative sample of the state (e.g., rural vs. urban, large vs. small). Our primary method of recruitment involved contacting stakeholders by telephone. Over 100 stakeholders were contacted, with 77 agreeing to participate (See Table 1). Efforts were made to ensure respondent confidentiality and anonymity. Participating stakeholders received an email survey. The survey contained detailed instructions, the scenario, and specific questions tailored to the stakeholder's setting. The questions were designed to drill down to the stakeholder's business practice. Email provided an

opportunity for stakeholder to attach applicable policies with their response. In many cases, the variation group members conducted a follow-up phone interview. In other instances, variation group members visited different professionals and conducted face-to-face interviews.

After the initial collection of business practices was complete, the formal VWG met to review the business practices and classify them as barriers to exchange or not. Additional business practices and clarifying questions emerged from these meetings. Follow-up on the business practices was completed by phone and by email. This completed the initial validation of our business practice data.

The LWG convened, as directed by RTI guidance, to identify state laws driving business practices identified as barriers. The LWG is in the process of completing an assessment of relevant state and federal regulations.

FINDINGS

Findings - Treatment Settings

Information use and disclosure for treatment, payment, and healthcare operations are understood and, while allowable under HIPAA without authorization, most providers still request patient authorization as part of the disclosure process.

Information transmission or exchange security protocols are in place, but vary by provider and stakeholder entity. There is a general acceptance of mail, but fax is the overriding practice. Some larger entities have the capability of automated encryption for email transmittal. Not everyone has secure email capability or trusts email transmission of PHI.

Differential application of 42 CFR Part 2 consent requirements and HIPAA provisions for use and disclosure is difficult to untangle. When does 42 CFR Part 2 apply and under what conditions?

In a treatment setting most healthcare professionals understand the HIPAA treatment, payment, and healthcare operations provision which provides for disclosure without patient authorization. Yet given that allowance, in a non-emergency situation providers or facilities will more often than not request that patient authorization be obtained as part of the disclosure process. The explanations for why this may occur include,

it may be required by the holder of the record, a defensive or protective measure against malpractice or privacy lawsuits, or good consumer-conscious practice. Transmission and exchange of information typically occur mostly by whatever means is most expedient given the situation. Healthcare providers across the state have a general familiarity with exchange partners' methods of communication and adapt to what is necessary to continue with treatment of the patient. In Utah, fax transmission is the most commonly used mode of transmission. In most long-term care facilities surveyed it is the only means for exchange. Many hospitals on the other hand have more sophisticated systems with automatic encryption when the string "PHI" is detected in the subject line of an email.

Scenario Review

Scenarios one through four describe four unique healthcare treatment events. Stakeholders were asked to discuss, given this specific situation, what would occur next, and how the exchange of patient health information would occur. The scenarios were used to promote a discussion regarding the exchange of information and identify business practices, across the responding stakeholder spectrum, regarding those exchanges.

Stakeholders - Treatment Scenarios

Hospitals

The majority of stakeholders responding to treatment scenarios one through four were hospital affiliated re-

Treatment Scenarios 1-4

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.

Treatment Scenarios (cont'd)

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 e-mail 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 e-mail.

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.

spondents (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 shows an overlap in community clinics and health centers that not only serve as homeless shelters, but also provide care for substance abuse and mental health patients. These respondents include the director of a private, non-profit program and the executive director at a state-licensed substance abuse treatment center. Also included in community clinic and health center respon-

dents 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 responding to scenario two receives a combination of government, private foundation, and individual contributions. Respondents for the public health agency include its director and a practicing physician assistant.

Clinicians

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

Long-Term Care Facilities

Respondents to scenario three representing the long-term care facility stakeholder group include the chief executive officer at a not-for-profit senior care facility and

the financial service consultant for rehabilitation and extended nursing care facility.

Variation - Treatment Scenarios

User and entity authentication

Little variation was reported across the treatment scenarios regarding business practices to verify that a person or entity that is seeking access to personal health information is who they claim to be. Hospitals, community clinics, and substance treatment facilities commonly accept a fax or mail request on letterhead as a form of authentication. In one hospital emergency room, the physician noted that when requests involve emergency situations, he asks for a national physician identification number. In addition, the emergency room physician uses the Internet to verify the facility is an actual facility. One treatment facility reportedly uses 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)]

Information authorization and access controls

In treatment scenarios one through four, the privacy and security domain listing the greatest number of business practices was information authorization and access controls (n = 15). It is 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 is granted with the least amount of difficulty to those working in an emergency medical environment. In those situations, security administration policies and procedures exist that allow an individual access to electronic and paper PHI based upon their role and responsibility. As the level of care and priority of treatment become less critical, access and authorization become 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 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.

In a long-term care facility, access to electronic and paper PHI is 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.

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 is at the discretion of the long-term care facility. Long-term care facilities operating electronic medical records require technical safeguards including unique user identification and procedures for accessing electronic PHI in an emergency. This would be true even if access were temporary. See 45 CFR § 164.514:(d)(2)(i); § 164.312.

Information use and disclosure

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 indicate that most covered entities prefer to

get patient authorization to disclose patient health information with the exception of an emergency situation. Business practice data show methods to account for disclosures.

Information transmission security or exchange protocols

Variation in transmission and security is evident among the major stakeholders in the health care community of Utah. Long-term care facilities use electronic fax as their method of choice for health information transmissions. Moreover, the hospitals, physician offices, and other major stakeholders use fax regularly but also use mail, courier, and patient pickup. The large hospitals and the integrated delivery systems have the ability to use encrypted email but this method is not yet widely used and accepted. Many facilities have policies in place that prohibit email use for transmitting patient information.

The sensitivity of the information being transmitted influences the security measures employed. On one extreme, substance abuse providers will verify the entity requesting patient information, ask the receiver to stand by the fax machine, stamp the fax cover sheet with “re-disclosure prohibited,” stamp the fax with the full CFR 42 Part 2 disclosure prohibition, and require a follow-up fax acknowledging receipt. Furthermore, one treatment facility reports that they require a signed receipt for anyone picking up patient records. These more stringent measures are in contrast with some physicians who report that they regularly disclose patient information over the phone once they are confident they are talking to an appropriate caregiver.

The physician can forward his or her own patient information to a specialist without patient authorization. Forwarding the treatment facility records would require patient consent to disclose to the specialist on the original disclosure or a new consent. When programs operating under Part 2 disclose information pursuant to a consent form, they must include a written statement that the information cannot be redisclosed. See 42 CFR § 2.32.

Mammography films are a unique case in Utah as the technology for digital mammograms has not been fully accepted and implemented. Until recently, most mammography clinics did not feel the resolution for electronic mammography films was adequate. 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 report rarely using these methods. It is more common to transfer films by person pickup with approved photo identification 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. The electronic methods (CDs and the Internet) are used commonly with other radiology films (e.g., x-rays) in Utah, especially among large facilities.

42 CFR Part 2 does not discuss transmitting PHI. Neither Utah State Code nor HIPAA specify the means or medium for transmitting PHI. However HIPAA does give general guidelines, including the following: 1. HIPAA requires covered entities to use appropriate administrative, technical, and physical safeguards to protect the privacy of PHI; and 2. HIPAA requires 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.

Administrative or physical security safeguards

Administrative or physical security practices to secure patient health information vary widely given the entity organizations and scenarios. Training in data security was noted as a requirement for each staff member, including volunteers at one responding hospital. Community clinic/public health agency employees and volunteers with direct access to patient charts records reportedly are required to sign confidentiality agreements prior to access.

Long-term care facilities and hospitals require 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 is at the discretion of the long-term care facility. Long-term care facilities operating electronic medical records require technical safeguards including unique user identification and procedures for accessing electronic PHI in an emergency. This would be true even if access were temporary.

Hospital safeguards are more electronic in nature and include passwords and security access cards. Access to the facility and to patient records is 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 tend to be paper-based and include locked and double locked doors. Substance abuse treatment facilities place a higher degree of sensitivity on the patient substance PHI reportedly placing it behind locked, double locked doors while immunization records are kept behind the nurse’s desk.

State Law Restrictions

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.

Critical Observations

Disclosure of patient health information is allowable for treatment, payment and healthcare operations without patient authorization. However most physicians in a treatment environment will opt to have the patient authorization before requesting the disclosure from another provider or covered entity.

42 CFR Part 2 and provisions for use and disclosure under HIPAA are difficult to untangle. The conditions and circumstances around application of 42 CFR and HIPAA "Treatment, Payment, and Healthcare Operations" for disclosure of patient information without authorization and patient consent to redisclose constrains exchange between treatment providers.

General precautions for transmitting patient health information are in practice. Though various procedures are employed, methods for exchanging between entities are commonly known in the provider community and transmittal is un-inhibited.

When an emergency room physician is dealing with an emergency situation and needs a patient's medical information, the physician will make efforts to access the patient's medical information without patient authorization. In emergency situations, hospitals will disclose information without authorization to a requesting covered entity once that entity is 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 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 report that in an

emergency, the information request would be fulfilled following authentication of the requestor. If not an emergency situation the practice is to have patient authorization to disclose.

There are differences between providers' treatment of patient medical information when substance use is involved. There is variation 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 note stringent precautionary measures to safeguard patient substance use information. While physicians comment on limited or restricted access to patient medical files, treatment facilities note that patient files are kept in a locked cabinet behind a double locked door.

There is 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 are 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 add to the confusion and misapplication of the regulation.

Long-term care facilities' have procedures in place to grant physicians temporary access to their facility and records system should temporary access be necessary. The policies and practice differ 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 is done by fax.

The majority of mammograms done in the state are on film; this is the case in both rural and urban facilities. One integrated delivery system currently uses digital images for mammography and a second has plans to transfer to digital within the next two years. However, even at the integrated delivery system that uses digital imagery, 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 to 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.

Findings - Payment

There is a common understanding among the payer community regarding the HIPAA “TPO” provision for use and disclosure of health information.

The “minimum necessary” standard is widely followed and while technology varies among the providers, the payers request access only to that which is necessary to accomplish their task.

Payers described the HIPAA provision that allows for the use and disclosure of patient health information without authorization. Many commented that authorization is often obtained at the practitioner level and that this is not something they as a payer would need to obtain separately.

It is clear that the payer and physician communities have worked to establish common language, understanding, and protections around the exchange of patient health information. Access to patient health information is granted with reliance that both entities are exchanging only that information necessary to achieve the task at hand.

Scenario Review

Scenario five depicts a payer-processing situation in which the payer is in need of additional information to approve and authorize patient encounters. In this situation, a case manager from the patient’s health plan seeks access to a provider’s patient electronic health record.

Stakeholders - Payment Scenario

Clinicians

A Health & Wellness Clinic responding as the clinician for scenario five specializes in the treatment of nerve, muscle and skeletal/spinal conditions. The clinic consists of component parts (chiropractic care, therapeutic massage and acupuncture) to offer a complete alterna-

tive health care approach. The clinic serves as a provider for most health insurance companies, as well as provides 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.

Consumer/Consumer Organizations

The consumer was a young mother who has changed jobs and has seen many different health insurance situations.

Variation - Payment Scenario

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 is given to the payer. How this happens varies based on the provider’s technological capabilities. In the case of an electronic record, special payment reports are created which give the payer only the information it needs. In a paper-based records environment, the information is 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 is noted in Utah concerning need for consent to disclose information when dealing with payment issues. The providers generally obtain a consent or authorization for payment purposes. Payers reported that they have access to health information under HIPAA “treatment, payment and healthcare operations” and that consent is not needed. The payers reported the necessity to have agreements in place in order to work

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.

with providers. The consumer believed that an authorization is required for patient information to be disclosed.

Critical Observations

Payers work with the understanding that patient authorization is not needed for payment purposes. Payers regularly engage in agreements with health care providers to facilitate the payment process. Health care providers show variation in whether 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 access patient and billing information varies. Both payers and providers report little variation in the description of what constitutes “minimum necessary” according to HIPAA.

Findings - Regional Health Information Organization (RHIO)

Utah's RHIO functions similar to a post office. It does not store, review, edit, or analyze the messages it transmits among its membership community.

Utah RHIO

The Utah Health Information Network (UHIN) is the dominant RHIO for the State of Utah. UHIN is a broad-based coalition of health care insurers, providers, and other interested parties, including the State of Utah Departments of Health and Insurance, and Medicaid Program. UHIN has established a centralized health data transaction system since 1994. UHIN is the hub for this system. This system coverage includes more than 450 third-party payers in the nation, 100% of hospitals, laboratories, Medicaid claims, local health departments and mental health centers in Utah and 85-90% Utah physicians/clinics and chiropractics. UHIN is a self-sustaining not-for-profit organization. All members sign a standard electronic commerce business agreement. It only charges enough to cover the costs of running the network.

UHIN Data Standards Committee plays a central role in Utah to implement and educate the community regarding HIPAA standards. In addition, the health care community through UHIN has developed a voluntary set of data standards for additional electronic transactions. The result is administrative simplification: one format for all the network users. A total of 34 UHIN Standards have become incorporated into Utah State rule via the Insurance Commissioner's Office.

UHIN also provides various training in health electronic commerce for its members. Their training courses include: privacy awareness, security, hands-on training for UHIN products, value of transactions, ASC X12N technical education, and business implications of electronic commerce.

In 2004 UHIN was awarded a five-year contract under the Agency for Healthcare Research and Quality (AHRQ) for \$5 million to expand UHIN's capability to act as a highway for clinical information. In addition, UHIN received a two-year contract from the Utah Department of Health to assist in the development of state-wide Bioterrorism reporting capability. Under these contracts

Utah is moving to create state of the art ability for both e-public health reporting and exchanging routine communications between health care providers to improve quality of care. It is the goal of the Utah Department of Health to build the best public health reporting capability in the nation.

Since 2004 UHIN has organized numerous community meetings to better understand the business case for exchanging clinical messages between health care providers and to begin to understand what would be involved in creating a real-time public health reporting system. All of the major health care stakeholders in Utah have been involved. UHIN is launching a pilot project to begin to develop and test these new exchanges.

Scenario Review

There are several models for implementing a RHIO. The RHIO scenario describes a situation where patient health data is monitored and used by the RHIO to track patient health needs and assess the provision of patient care.

Stakeholders - RHIO

Consumer/Consumer Organizations

The RHIO responding to scenario six is a non-profit coalition of competing entities that provide secure, electronic information exchange connecting every payer and nearly every healthcare provider in the state of Utah. It operates as a "gateway" or "information highway" exchanging information between different entities. The RHIO does not view, store, edit, or evaluate the quality of data it receives. Instead, the Utah RHIO functions like a "post office" transferring information from the sender to the intended receiver.

Critical Observations

This 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 members' 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.

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.

Findings - Research Data Use

Institutional Review Board (IRB) process is a defined procedural process with clear guidelines for submission and conditions for re-submission. The principal investigator has some discretion in determining whether to resubmit to IRB. This decision can be affected by the content of the original patient authorization and consent, as well as the secondary analysis.

Scenario Review

This scenario presents a research study that has cleared the IRB process. A secondary researcher requests to use of the data for another research project that will result in a white paper.

Stakeholders - Research Data Use

Clinician

Of the two research investigators responding to scenario seven, one is 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 employs this individual.

Physician Groups

The second researcher responding to scenario seven is a licensed pediatrician with a university-affiliated practice that also serves as assistant professor of pediatrics. A medical and public health school that undertakes research employs 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 serves as the senior compliance consultant of an integrated delivery system. Both respondents have numerous years of experience serving on institutional review boards.

Consumer/Consumer Organizations

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

Variation - Research Data Use

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 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.

Critical 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 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 also noted in the requirement of a parental re-consent and a study subject re-assent for the use of data beyond that originally included in the protocol approved by IRB. One researcher indicated that approval is required while a second indicated that they would first search for prior authorization. More variation is demonstrated by the IRB suggestion that the project be submitted data-only and thereby negating the need for a re-consent and re-assent.

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.

Findings - Access By Law Enforcement

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.

A disconnect exists between law enforcement and healthcare. Hospitals are a covered entity and respond accordingly for the use and disclosure of information to law enforcement. Law enforcement operates according to State and county regulations. Communication, sharing and exchange between these two organizations is difficult. In many cases the two speak different languages and the result is a very formal and lengthy process that requires legal documentation to permit the exchange.

Scenario Review

The following scenario describes law enforcement and hospital emergency room staff following a traffic accident. The driver in question is suspected of using alcohol and causing the accident. The interaction between hospital emergency room staff and law enforcement is an every day event. The exchange of information between these two entities, given this situation is a formal process that involves lengthy paperwork and extensive time.

Stakeholders - Access by Law Enforcement

Hospitals

Representing the hospital stakeholder for scenario eight is 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 variations work group 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 is 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, eight, and 13. Another respondent to scenario eight is currently 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 is being viewed in the household.

Variation - Access to Law Enforcement

Information use and disclosure

Most of the business practices in scenario eight focus on disclosing patient health information. A clear chasm exists between law enforcement and the medical community that prohibits the exchange of information. Law enforcement reports that they have officers collect as much information as possible prior to transporting an individual to a hospital. This is a necessary operating procedure because once the individual enters a medical facility the difficulties law enforcement experience in gathering information increase significantly. In addition, from a law enforcement perspective, most physicians

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.

are reluctant to talk because they don't want to be involved in any legal proceedings.

Most physicians report they cannot disclose patient information without legal documentation to do so or the patient's authorization.

Critical Observations

Scenario eight highlights the chasm that exists 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 is believed to stem from a desire to avoid legal entanglements. Similarly, hospital physicians are very careful not to disclose information to parents and instead will opt 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 are different from those of a paramedic, which adds another layer of complexity. Most law enforcement agencies will maintain business agreements with paramedics to perform blood alcohol draws at the scene of an accident and law enforcement is adamant that officers gather as much information as possible before the patient gets to the hospital. The reason for this is identified as being a result of little, if any, information being gathered after the patient enters the hospital without initiating legal paperwork.

Findings - Prescription Drug Use/Benefit

Business associate agreements are reported as a common practice and are in place regardless of whether they are required. This was true with the exception of entities using de-identified data. Though not all responding stakeholders reported having the agreements as the exchange was allowed under HIPAA's "TPO", for those that did they felt it was good practice.

Scenario Review

The following two scenarios describe pharmacy benefit manager interactions in two situations: 1) the filling of prescription through mail order and 2) a company conducting a cost comparison of benefits. Little variation exists in collected business practices for these scenarios.

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 intimate nature of the practice and the fact that the practitioner owns the practice may have resulted in a response considered above and beyond what may normally be expected with regards to patient communication.

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.

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.

Stakeholders - Prescription Drug Use/Benefit (A & B)

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, IV, in home and outpatient pharmacy services.

Variation - Prescription Drug Benefit/Use

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 may each use or disclose protected health information for their own treat-

ment, 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 deidentified/aggregated information be provided if that is sufficient to carry out PBM1’s assignment. See 45 CFR § 164.514(d).

If only deidentified 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 non-disclosure agreement). These additional contracts are not required by HIPAA

Critical Observations

In scenario nine, variation is 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 will contact the patient and in other cases it is 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 exists in scenario ten with regards to whether a business associate agreement is 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.

Findings - Healthcare Operations and Marketing

Health care entities report little to no marketing activity as defined under HIPAA. Patient education and promotion of care occur through internal departments. No entity responding to either healthcare operations and marketing scenario engages in the selling of patient data.

Scenario Review

Two scenarios (11 and 12) provide information around the circumstances for which a health care operation uses patient information to inform consumers about educational opportunities as well as market new services.

Stakeholders - Healthcare Operations and Marketing

Hospitals

Answering as a hospital stakeholder for scenario eleven is 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 is 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 is a medical doctor who was a practicing obstetrician until closing this practice within the last year. This physician is now employed by a consumer organization and currently serves on many administrative panels locally and nationally.

Consumer/Consumer Organizations

Two respondents answered as consumers to scenario twelve and included an individual employed as a marketer for a pharmaceutical corporation and a patient advisor for a cancer education network.

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.

Variation - Healthcare Operations and Marketing

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 does 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 would not require patient authorization.

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

One hospital responded that it transmits 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 exists is due largely to what the activity is and whether the hospital views it as a marketing activity. Most of the purposes depicted in the scenarios do not constitute marketing according to the definition of marketing. See 45 CFR § 164.501. Most facilities that responded to the Healthcare Marketing and Operations by making a distinction in the purpose and intent for using patient information according to whether the information was used: 1. To inform, which is not marketing; or 2. To promote, which is marketing. The activity depicted in scenario eleven would not constitute marketing but two of the four in scenario twelve, fund-raising and selling data, require patient au-

thorization for the use of their information. See 45 CFR § 164.514 (f)(1); § 164.508 (a)(3).

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 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).

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 provides 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.

Findings- Bioterrorism Event

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 Review

The following scenario describes a suspected anthrax exposure. The scenario begins with the physician that orders the patient lab work and quickly involves other agencies and organizations in a collaborative effort to a potential Bioterrorism event.

Law Enforcement

One individual representing the law enforcement stakeholder group is 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, eight, and 13. Another respondent to scenario eight is currently 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

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.

Stakeholders - Bioterrorism event

Physician Groups

The physicians responding to scenario thirteen are a semiretired obstetrician, a general practitioner who serves 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.

Other (Fire Department)

One respondent is a fire fighter serving in a district that is currently structured under the umbrella of Public Safety. The department employs 39 full-time fire fighter/ EMT/paramedics and one part-time secretary and houses the Training and Operations Chief.

Variation - Bioterrorism Event

State Law Restrictions

All health care providers are 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 dis-

eases is pursuant to The Communicable Disease Act found in Utah Code § 26-6. The provisions of Utah Code § 26-23b specifically apply to the reporting of information that might indicate a bioterror event. HIPAA allows for public health reporting without patient authorization. It allows for both voluntary and mandatory disclosures to public health. See 45 CFR §164.512. HIPAA also allows 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 has two provisions dealing with disease reporting. The general reporting statute is 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 implements these statutes is R386-702. Anthrax is listed among the reportable diseases.

Covered entities may share PHI with law enforcement as provided in 45 CFR § 164.512(f) and (k). The HIPAA regulations do not apply to health information while it is held by an entity that is not a covered entity. Public health agencies are 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 may use personally identifiable health information. State law controlling public health agencies allows them to share information with law enforcement but is 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 is more restrictive than the emergency disclosure provision of 42 CFR § 164.512(j).

Critical Observations

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

Findings - Employee Health

Employers did not feel access to an employee's electronic health record was necessary. The information employer's request for a "return to work" document is general statements about an employee's condition and their ability to work with or without restriction.

Electronic transmission of a "return to work" document is not a practice in the state. The preferred reported delivery is by the employee. Some hospitals and physicians indicate they would mail the document at the request of the patient.

Scenario Review

In the following scenario the employee has been out of work for four days due to illness and per employer policy is not permitted to return unless cleared by a physician. The employer requires that the employee provide a "return to work" document prior to the employee returning to work.

Stakeholders - Employee Health

Hospitals

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

Consumer/Consumer Organizations

A director of development at a local company that is self insured responded on behalf of the consumers in this scenario. The company is 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.

Variation - Employee Health

There were no reports of variation in the way hospitals handle "return to work" documents. We heard of 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 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.

Critical Observations

Hospitals responding to the 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.

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.

Findings - Public Health Scenarios

Public health and healthcare entities function under different rules for exchanging patient health information. The public health agencies are afforded more flexibility for the use of health information. Public Health is diligent in its efforts to protect the privacy of the individual. Public health information exchanges with law enforcement are guarded and occur at the discretion of the public health officials.

Scenario 17 Public Health C did not apply to our state. Utah does not operate county shelters nor hospital-affiliated drug treatment clinics. The homeless are treated in social-based, not medical-based, facilities. It is rare that a homeless person would have a primary care provider.

Scenario Review

The public health scenarios take into account three separate situations: 1) an active, multi-drug resistant tuberculosis patient that has boarded a bus out of state without notifying officials; 2) the tracking and procedure for a positive result on a newborn screening; and 3) county-provided drug treatment services for a homeless individual.

Stakeholders - Public Health (A, B & C)

Clinicians

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

Physician Groups

One physician responding to scenario 17 is a family practitioner employed by a health center that is part of a larger integrated delivery system. The physician responding to scenarios 16 and 18 is 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 is the executive director

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 addition 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.

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, is a physician serving as the medical director. The other respondent, representing the state-owned laboratory and further employed by a genetic collaborative center, provides current and ongoing education regarding newborn screening to practitioners and consumers and maintains quality in delivery of newborn screening services.

State Government (Public Health Departments)

Representing the state government public health department, is the manager of a data integration program that specializes in linking child health information from several programs which currently include: Vital Records (Birth and Death Certificates), USIS (Utah Statewide Immunization Information System), Newborn Hearing Screening and Baby Watch/Early Intervention. Future developments for the data integration program will include the Newborn Screening (heelstick) program and the Birth Defects Network.

Law Enforcement

One individual representing the law enforcement stakeholder group is a detective that served on the variations work group. Another respondent to scenario 15 is currently Chief of Police for a town with a population of less than 15,000.

Consumer/Consumer Organizations

Consumer responses to scenario 15 and 17 are 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.

Variation - Public Health (A,B &C)

State Law Restriction

In the case of scenario 15, Utah requires that all health care providers 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 is pursuant to The Communicable Disease Act found in Utah Code § 26-6. HIPAA allows for public health reporting without patient authorization. It allows for both voluntary and mandatory disclosures to public health. See 45 CFR § 164.512. HIPAA also allows a covered entity to disclose PHI without authorization when necessary to avert a serious threat to health or safety. See 45 CFR § 164.512.

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

HIPAA DOES NOT GOVERN PUBLIC HEALTH COMMUNICABLE DISEASE INTERVENTION.

Communicable disease prevention activities of public health agencies are not covered functions under HIPAA. HIPAA does 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 may 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 allows disclosure of all records that state law requires to be disclosed. See Utah Code § 26-6b-3.4. Medical records — Privacy protections; 45 CFR § 164.512.

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

The Government Records Access and Management Act (GRAMA) does 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 provides that records that are classified under a different statute or by federal law are to be governed by the other law. The method that the public may use to obtain access to public health records may still be governed by GRAMA. Protected health information held by a Utah governmental entity that is a covered entity subject to HIPAA are not governed by GRAMA.

nosis and the state will contact the parents in addition to the physician.

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 rare that a homeless person would have a primary care provider.

Critical Observations

As noted in previous scenarios, general precautions for transmitting patient health information are in practice. 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.

Utah does not notify specialty care centers (as described in scenario sixteen) unless there are critical results as agreed upon with the specialist. Utah also does 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 patients can be tracked through a Metabolic Clinic however. Medical homes and families are notified of eligibility for this clinic upon diag-

Findings - Health Oversight/ Government Compliance And Accountability

The various entities named in this scenario involved in Health Oversight are not all subject to the same restrictions regarding release of the data. For example, Medicaid is a “covered entity” and will be subject to HIPAA regulations. The public health authority is not a covered entity and is governed by state law not HIPAA.

Scenario Review

The following scenario refers to developing a centralized database to track health indicators, at the governor request. It entails collaboration between several different state government agencies and the state university to monitor and track blood lead levels and childhood immunizations. The governor hopes that identification of migration patterns between states and tracking childhood immunizations and blood lead screening will improve healthcare for low-income children.

Network. Also responding for the state public health department with regards to scenario 18 are state program directors.

Medical and Public Health Schools that undertake Research

Representing a medical and public health school that undertakes research is a licensed pediatrician with a university-affiliated practice that also serves as assistant professor of pediatrics.

Variation - Health Oversight

For Medicaid, a release of data to the university might be part of HIPAA “TPO” if Medicaid requires analysis of lead or immunizations. Authorization for the release would not be required. See 45 CFR § 164.506 (c)(1). If that is the case, it would be necessary for Medicaid to have a business associate agreement with the univer-

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.

Stakeholders - Health Oversight

State Government (Public Health Departments)

For the State Government Oversight, representing the state government public health department, is the manager of a data integration program that specializes 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. Future developments for the data integration program will include the Newborn Screening (heelstick) program and the Birth Defects

city. See 45 CFR § 160.103(B)(ii); § 164.504. The university would not be allowed to redisclose the information obtained through the business associate agreement unless such redisclosure was part of the contract.

If the release of the data were not part of TPO it would require 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 is not subject to HIPAA but will be subject to the confidentiality requirements of U.C.A. § 26-1-17.5 “ A record classified as confidential under this title shall remain confidential and be released

according to the provisions of this title.” The lead data is collected pursuant to R386-703 (1)(h) and is confidential pursuant to R 386-703-6(1) and could not be released except with a “written consent of the individual.” See U.C.A. § 26-6-27 (2)(a).

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

Critical Observations

The Department of Health maintains the Utah State Immunization Information Systems (USIIS) that holds records of children’s immunizations. Only authorized health care users have access to USIIS. Approximately 130 of 350 provider offices have enrolled with user confidentiality to have access. Office staff of participating providers can access USIIS through an enrollment process that requires annual renewal. Terminated or released staff lose access privileges to USIIS access. A “look up only” access is granted to researchers that have a legitimate research purpose and IRB approval. Utah also added lead poisoning to the injury surveillance and reporting system in 1990 per Utah Code R386 - 703 (Injury Reporting Rule).

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. 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.

CONCLUSION

Interoperability in healthcare systems has the potential to provide many benefits, including improved quality of care, more timely and thorough public health disease and bioterrorism event surveillance, and cost containment. Defining interoperability can be a challenge. Interoperability is a multifaceted concept. As a general notion, it is the ability of information systems to work together within and across boundaries to effectively exchange and use information. Promoting the use of common information technologies through interoperable systems and standards will improve outcomes and reduce costs by improving efficiency. In addition, the ability to easily share and exchange information makes possible a powerful resource against bioterrorism, the spread of disease, and other homeland security concerns.

The question then is: What access is needed for law enforcement and public health in an interoperable healthcare system? Utah's healthcare system operates 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. A clear goal that defines Utah's e-Health system can clarify the participants that need to be involved in designing the system. This may include health insurers, physicians, hospitals, state health departments, local health departments, pharmacies, law enforcement, and public schools.

To achieve cooperation, it is important to understand the stakeholder roles and how their applicable governing requirements fit into an interoperable system. Maximizing the benefits of interoperability and maintaining the individuals right to privacy and security requires a clear working definition with achievable goals. All stakeholder entities must become part of the discussion and as we move forward in defining what an interoperable healthcare system means for Utah.

The absence of understanding and clarification of the regulatory requirements governing agencies and partners exchanging health information impedes the flow and exchange process. Different terminology and concepts increase the difficulty in communication, sharing and the exchange of information, which in turn can negatively impact the quality of care. The confusion that exists within the healthcare community regarding sensitive health information can lead to that information which the physician may need to render adequate care being filtered out of the record transmission.

Some providers work with a general understanding of

HIPAA, its provisions and allowances for data use and disclosure, and minimum necessary standard. When a provider engages in the exchange and transfer of information outside HIPAA, the difficulty increases significantly. The exchange is anything but a seamless and barrier free process. Law enforcement and public health exchanges with covered entities are formal cumbersome procedures.

The importance of healthcare connectivity in a 21st century global environment cannot be minimized. To avert public threats, bioterrorism, and conduct public health surveillance requires that public health and law enforcement access health information. Traditional public health surveillance and investigations involves timely manual reporting of cases to public health agencies and phone calls to healthcare providers for more detailed patient chart information. The process can be problematic and too slow to be effective during a public health emergency. The value of exchanging existing health data electronically in a standardized format provides a unique opportunity to leverage those existing health data to better support public health functions of disease detection, monitoring, and real-time situational awareness.

NOTES

1 The Utah Digital Health Service Commission is an eleven member public-private commission appointed by the governor. See Utah code 26-9f-104.

2 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.

3 HealthInsight is participating in several other health information technology projects. HealthInsight 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 is Scott Williams, MD who also serves as the VP, Medical Affairs for HealthInsight. HealthInsight is also responsible for the evaluation of that grant, is leading a subgroup to involve practicing physicians and 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. Funding for this project has been provided by the CDC and AHRQ. 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.

4 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.