

## TABLE OF CONTENTS

<b>Table of Contents</b> .....	<b>1</b>
<b>Analysis of Scenario #1</b>	
<b>Patient Care - Scenario A</b> .....	<b>7</b>
Scenario Overview .....	7
General Business Processes in Addressing the Scenario .....	8
Necessity of the Information .....	8
Requesting and Exchanging Information .....	8
Providing Information .....	8
Impact of Key Issues .....	9
Variations in Business Practice .....	9
Application of the Project Privacy and Security Domains .....	10
User and Entity Authentication .....	10
Key Issues .....	10
Business Practice Variation .....	11
Information Authorization and Access Controls .....	11
Information Audits that Record and Monitor Activity .....	12
State Law Restrictions .....	12
Key Issue .....	12
Business Practice Variation .....	12
Legal Issues .....	12
Identified Barriers or Best Practices .....	13
<b>Analysis of Scenario #2</b>	
<b>Patient Care - Scenario B</b> .....	<b>14</b>
Scenario Overview .....	14
General Business Processes in Addressing the Scenario .....	15
Exchanging Substance Abuse Treatment Information .....	15
Internal Handling and Use of Substance Abuse Treatment Information.....	15
Impact of Key Issues .....	16
Variations in Business Practice .....	16
Application of the Project Privacy and Security Domains .....	16
Information Audits that Record and Monitor Activity .....	16
Key Issue .....	17
Administrative or Physical Safeguards .....	17
State Law Restrictions .....	18
Identified Barriers or Best Practices .....	18
<b>Analysis of Scenario #3</b>	
<b>Patient Care – Scenario C</b>	
<b>Security and Access</b> .....	<b>19</b>
Scenario Overview .....	19
General Business Processes in Addressing the Scenario .....	20

Providing Health Information to Visiting Physicians..... 20  
 Exchanging Summaries and Use of Transcription Services ..... 21  
 Impact of Key Issues ..... 21  
 Variations in Business Practice ..... 22  
 Application of the Project Privacy and Security Domains ..... 22  
 Identified Barriers or Best Practices ..... 22

**Analysis of Scenario #4**

**Patient Care - Scenario D..... 23**  
 Scenario Overview ..... 23  
 General Business Processes in Addressing the Scenario ..... 24  
     Exchanging/Disclosing HIV-Related Health Information..... 24  
     Exchanging/Disclosing Genetic Health Information ..... 25  
     Exchanging/Disclosing Digital Images ..... 25  
     Impact of Key Issues ..... 25  
     Variations in Business Practice ..... 26  
 Application of the Project Privacy and Security Domains ..... 26  
     Patient and Provider Identification ..... 26  
     Information Transmission Security or Exchange Protocols ..... 27  
     Administrative or Physical Safeguards ..... 27  
     State Law Restrictions ..... 27  
 Identified Barriers or Best Practices ..... 28

**Analysis of Scenario #5**

**Payment Scenario..... 29**  
 Scenario Overview ..... 29  
 General Business Processes in Addressing the Scenario ..... 30  
     Granting Health Plans/Payers Access to Electronic Health Records ..... 30  
     Providing Health Information for Pre-Authorization ..... 30  
     Impact of Key Issues ..... 31  
     Variations in Business Practice ..... 31  
 Application of the Project Privacy and Security Domains ..... 32  
     Information Audits That Record and Monitor Activity ..... 32  
     State Law Restrictions ..... 32  
 Identified Barriers or Best Practices ..... 33

**Analysis of Scenario #7**

**Research Data Use..... 34**  
 Scenario Overview ..... 34  
 General Business Processes in Addressing the Scenario ..... 35  
     Definition of Research Versus Quality Assessment..... 35  
     Research Protocols Reviewed by an Institutional Review Board ..... 36  
     Use of De-Identified Data ..... 36  
     Use of Individually Identifiable Health Information ..... 36  
     Primary Data Collection, Storage and Use ..... 37  
     Secondary Data Extraction, Storage and Use..... 37  
     Exchanging Data with External Researchers ..... 37



Impact of Key Issues ..... 38  
 Variations in Business Practice ..... 38  
 Application of the Project Privacy and Security Domains ..... 39  
     Information Audits That Record and Monitor Activity ..... 39  
 Identified Barriers or Best Practices ..... 39

**Analysis of Scenario #8**

**Access by Law Enforcement ..... 40**  
 Scenario Overview ..... 40  
 General Business Processes in Addressing the Scenario ..... 41  
     Providing Information ..... 41  
     Impact of Key Issues ..... 41  
     Variations in Business Practice ..... 42  
 Application of the Project Privacy and Security Domains ..... 42  
     Information audits that record and monitor the activity ..... 42  
     Administrative or physical safeguards ..... 42  
     State Law Restrictions ..... 42  
 Identified Barriers or Best Practices ..... 43

**Analysis of Scenario #9**

**Pharmacy Benefit - Scenario A ..... 44**  
 Scenario Overview ..... 44  
 General Business Processes in Addressing the Scenario ..... 44  
     Exchanging Prescription Drug Data ..... 44  
     Addressing Formulary Issues ..... 45  
     Linking Electronic Health Records to Health Plan Formularies ..... 46  
     Impact of Key Issues ..... 46  
     Variations in Business Practice ..... 46  
 Application of the Project Privacy and Security Domains ..... 47  
     State Law Restrictions ..... 47  
 Identified Barriers or Best Practices ..... 47

**Analysis of Scenario #10**

**Pharmacy Benefit - Scenario B ..... 48**  
 Scenario Overview ..... 48  
 General Business Processes in Addressing the Scenario ..... 49  
     Exchanging Claims Data with a PBM..... 49  
     Method for Exchanging Data ..... 49  
     Impact of Key Issues ..... 49  
     Variations in Business Practice ..... 49  
 Application of the Project Privacy and Security Domains ..... 50  
     State Law Restrictions ..... 50  
 Identified Barriers or Best Practices ..... 51

**Analysis of Scenario #11**

**Healthcare Operations and Marketing - Scenario A..... 52**  
 Scenario Overview ..... 52



General Business Processes in Addressing the Scenario ..... 53  
     Using Individually Identifiable Health Information for Health Care Operations..... 53  
     Limiting Use of Health Information..... 53  
     Impact of Key Issues ..... 54  
     Variations in Business Practice ..... 54  
 Application of the Project Privacy and Security Domains ..... 54  
 Identified Barriers or Best Practices ..... 54

**Analysis of Scenario #12**

**Healthcare Operations and Marketing - Scenario B..... 55**  
 Scenario Overview ..... 55  
 General Business Processes in Addressing the Scenario ..... 56  
     Using Individually Identifiable Health Information for Health Care Operations..... 56  
     Using Individually Identifiable Health Information for Fundraising..... 57  
     Using Individually Identifiable Health Information for Marketing ..... 57  
     Exchange of Birth Information..... 58  
     Impact of Key Issues ..... 58  
     Variations in Business Practice ..... 59  
 Application of the Project Privacy and Security Domains ..... 59  
     Information Audits that Record and Monitor Activity ..... 59  
 Identified Barriers or Best Practices ..... 59

**Analysis of Scenario #13**

**Bioterrorism Event..... 61**  
 Scenario Overview ..... 61  
 General Business Processes in Addressing the Scenario ..... 61  
     Disclosure of Health Data in General ..... 62  
     Disclosure of Health Data to Health Care Providers and Local Public Health ..... 63  
     Disclosure of Health Data to Law Enforcement ..... 64  
     Disclosure of Health Data to Others ..... 64  
     General Privacy Concerns ..... 64  
     Impact of Key Issues ..... 65  
 Application of the Project Privacy and Security Domains ..... 65  
 Identified Barriers or Best Practices ..... 65

**Analysis of Scenario #14**

**Employment Information ..... 66**  
 Scenario Overview ..... 66  
 General Business Processes in Addressing the Scenario ..... 67  
     Creation and Content of Letter to an Employer ..... 67  
     Transmission of Letter to an Employer ..... 67  
     Follow-Up Discussions with an Employer ..... 68  
     Impact of Key Issues ..... 68  
     Variations in Business Practice ..... 68  
 Application of the Project Privacy and Security Domains ..... 69  
     State Law Restrictions ..... 69  
 Identified Barriers or Best Practices ..... 69



**Analysis of Scenario #15**

**Public Health - Scenario A**

**Active Carrier, Communicable Disease Notification..... 70**

- Scenario Overview ..... 70
- General Business Processes in Addressing the Scenario ..... 70
  - Disclosure of Health Data in General ..... 71
  - Exchanging Health Data with the Patient’s Physician..... 71
  - Disclosing Health Data State B ..... 72
  - Disclosing Health Data to Other States ..... 72
  - Disclosing Health Data to the Bus Company ..... 72
  - Accessing Health Data through Electronic Health Records..... 73
  - Impact of Key Issue ..... 73
- Application of the Project Privacy and Security Domains ..... 73
- Identified Barriers or Best Practices ..... 73

**Analysis of Scenario #16**

**Public Health - Scenario B**

**Newborn Screening ..... 74**

- Scenario Overview ..... 74
- General Business Processes in Addressing the Scenario ..... 75
  - Newborn Screening Background ..... 75
  - Exchange of Presumptive Positive Screening Results with Providers..... 75
  - Disclosure of Health Data to Law Enforcement ..... 76
  - Disclosure of Health Data to Others ..... 76
  - Connection to Social Services and Other Programs ..... 76
  - Impact of Key Issues ..... 77
- Application of the Project Privacy and Security Domains ..... 77
  - User and Entity Authentication ..... 77
- Identified Barriers or Best Practices ..... 78

**Analysis of Scenario #17**

**Public Health - Scenario C**

**County Programs for Chemical Dependency ..... 79**

- Scenario Overview ..... 79
- General Business Processes in Addressing the Scenario ..... 79
  - Exchange of Individual-Identified Data during Assessment ..... 80
  - Exchange of Individual-Identified Data after Assessment ..... 80
  - Disclosing Individual-Identified Health Data to Others..... 81
  - Impact of Key Issues ..... 81
  - Variations in Business Practice ..... 82
- Application of the Project Privacy and Security Domains ..... 82
- Identified Barriers or Best Practices ..... 82

**Analysis of Scenario #18**

**Health Oversight**

**Legal Compliance/Government Accountability ..... 83**

- Scenario Overview ..... 83



General Business Processes in Addressing the Scenario ..... 84

- Disclosure of Medicaid Data ..... 84
- Disclosure of Blood Lead Surveillance System Data ..... 84
- Disclose of Immunization Registry Data ..... 85
- Centralization of Data from All Sources..... 85
- Linking of Individual-Identifiable Data ..... 86
- Accessing Data Directly from an Electronic Health Record..... 86
- Impact of Key Issues ..... 87
- Application of the Project Privacy and Security Domains..... 88
- State Law Restrictions ..... 88

Identified Barriers or Best Practices ..... 88



## ANALYSIS OF SCENARIO #1 PATIENT CARE - SCENARIO A

---

### SCENARIO OVERVIEW

---

*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. 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 inpatient stay.*

To provide structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified three key issues and seven questions for consideration (see Expanded Scenario #1). The three key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The identified issues were:

- **Emergency Treatment:** This issue was identified as a key issue, because it was anticipated that the processes used in emergency situations differ from the processes used in non-emergency situations, where the timing of the exchange may be less critical. In addition, Minnesota law allows health care providers to release health information for a medical emergency when the provider is unable to obtain the patient's consent due to the patient's condition or the nature of the medical emergency.
- **Mental Health Records and Information:** This issue was identified as a key issue, because it was anticipated that some health care providers' policies may provide added privacy protections to mental health records. Many patients are concerned about the release of their mental health records and it was thought that this concern might be reflected in the policies related to the exchange of this information.
- **Cross-State Health Information Exchange:** This issue was identified as a key issue for two reasons. First, it highlights that the exchange of information may be occurring between institutions that do not regularly have a need to exchange information. Second, this project plans to have regional meetings with our neighboring states (i.e., Wisconsin and Iowa) to identify and address barriers to cross state information exchanges. Thus, this issue was included to begin identifying those barriers.

The seven questions for consideration were intended to focus the work group's discussion, as well as to provide slight modifications to the scenario. The scenario is very specific and likely to evoke very specific, fact-dependent business processes. In order to have a more complete discussion of the scenario, we introduced small changes to the facts of the scenario in an effort to identify their impact on the business processes related to the exchange of the information. The seven questions attempted to:

- Elicit the business processes used in trying to obtain the health information
- Elicit the business processes used if requested to provide the health information to another hospital
- Determine the importance of the fact that this is being described as emergency treatment

- Determine the importance of the fact that the health information is mental health information
- Identify any differences in the business processes used in exchanging health information across state borders versus within state borders
- Identify any differences in the business processes used in exchanging health information with other hospitals versus a medical clinic that has a routine relationship with the hospital
- Describe the intersection of the scenario with the nine privacy and security domains used within the project

---

## GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

### Necessity of the Information

The Variations Work Group did not consider this scenario's health information exchange to be a common situation for information exchange and questioned the need for the information. Because the scenario is situated in the emergency room, the first focus of the hospital would be on stabilizing the life of the patient and addressing any trauma from the car accident. It was stated that diagnoses and treatment information would only be requested if it were necessary to stabilize the life of the patient. Work group members generally believed that the diagnoses and treatment information would be solicited after the patient was stabilized and admitted to the hospital.

One of the Variation Work Group members whose organization's electronic health record is available to physicians in the emergency room indicated that if the patient were in the emergency room and if there was diagnosis and treatment information available, then the physician would consult the information. Thus, it appears that when the information is readily available it is consulted and used. However, when the information is not readily available and is not needed to stabilize the patient, it would generally not be requested, consulted, or used until later in the care process.

### Requesting and Exchanging Information

The Variation Work Group members were unanimous in stating that when confronted with the situation of Scenario #1, the request and exchange of health information would be done through telephone and fax. A physician or nurse from the emergency room would telephone the other hospital, identify themselves, describe the situation, identify the patient, and request the needed information. If the other hospital is willing and able to supply the information, it would generally be provided in one of two ways: 1) A provider-to-provider discussion over the telephone; or 2) The information would be faxed to the emergency room. There appeared to be no variation in how the information would be requested and exchanged.

### Providing Information

The work group was also asked to identify the business processes used when their organization is asked to supply health information to another hospital in the situation described in the scenario. The Variations Work Group Members were unanimous in stating that the biggest difference between providing the requested information and requesting to be provided the information is the responsibility for ensuring the appropriateness of the disclosure or release of information. That is, the organization providing the health information has the responsibility for ensuring the appropriateness and legality of any health information disclosed or exchanged. The consequences of the responsibility for the appropriateness of the exchange is manifest in their attention to the details of what information is being disclosed, verifying the recipient's identity, determining the need for a consent to disclose the information, and documenting the disclosure.

### Impact of Key Issues

**Emergency Treatment** was not considered a key issue when requesting the information, although it was considered a key issue when being asked to provide the information. Variation Work Group members pointed out that, in general, they need to have consent to authorize the disclosure of health information. However, Minnesota law permits a health care provider to release health information for a medical emergency when the provider is unable to obtain the patient's consent. Thus, work group members believed that they would be able to legally disclose the information being requested in this scenario.

In determining the appropriateness of disclosing the information, work group members described the need to balance patient risk with organizational risk. Patient risk is the threat to the patient that results from not disclosing information urgently needed to stabilize the patient's condition. Organizational risk is the legal risk to the health care provider or organization for inappropriately disclosing or inappropriately documenting the disclosure of health information. It is the balancing of these two risks that creates variations between organizations.

Most work group members indicated that they would initially request consent authorizing the disclosure of the requested information. When presented with information and evidence that the situation was an emergency and that patient consent would not be possible, most work group members indicated that they would disclose the information. At least one organization indicated that given the facts of this specific scenario that their organization would probably insist on obtaining consent before disclosing the information. Other work group members also indicated that determining when to disclose information without consent is very situation specific, and depending on the situation, may require the involvement of the organization's Health Information Manager or Privacy Officer.

Although **Mental Health Records** were part of the scenario, they did not generate variation in the processes used to obtain or provide the relevant health information. Work group members generally believed that the mental health records were relevant to the patient's condition and could be related to the patient's confusion. One work group member noted that the State of Wisconsin requires a specific authorization (see Wisconsin Statutes § 51) for the disclosure of mental health records. Consequently, it is possible that a Minnesota hospital attempting to acquire mental health records could face barriers or delays by being unfamiliar with the other state's specific requirements.

The **Cross-State Exchange of Health Information** was not viewed as a key aspect in the scenario. The work group members indicated that their processes would be the same regardless of whether they were exchanging the information with a hospital in another state, another Minnesota hospital, or a clinic with whom they had regular dealings.

### Variations in Business Practice

In general, there were few variations in the business policies and practices used by Variations Work Group members in obtaining or providing the health information related to the scenario. Given that the exchange of information anticipated by the scenario is almost always conducted via telephone or fax, it is not surprising that the practices are nearly identical. The only real variation was related to how organizations balanced patient risk with organizational risk when making the decision to provide health information without the patient's consent. While most organizations indicated that they would be willing to provide the requested information without consent, at least one organization stated that they would probably require patient consent prior to disclosing this information.

## APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario, including the modifications addressed in the questions for consideration. Recognizing that the exchange contemplated by the scenario occurs almost exclusively by telephone and fax, work group members were also asked to describe issues that would arise if this exchange were to be conducted electronically between organizations.

### User and Entity Authentication

Variations Work Group members identified the issue of user and entity authentication as an important issue in situations where their organization was being asked to provide health information. All work group members indicated that their organization had a protocol for verifying the entity requesting the information. While there may be slight variations across organizations, all of the organizations used some combination of the following methods:

- Use of Caller ID to identify the origin of the caller requesting the information
- Asking the caller requesting the information for a telephone number to verify that the number matches the Caller ID and to contact the requester
- Asking for the main telephone number of the hospital and an extension where the requester may be contacted within the hospital
- Asking that the request for information be faxed on hospital letterhead
- Asking for the UPIN number or National Provider Identifier (NPI) for the physician requesting the information

Work group members pointed out that because the situation described in the scenario would require provider-to-provider interaction over the phone, providers would be able to use their judgment as well as the above-described authentication methods. Two physicians or nurses interacting over the phone would be able to judge the legitimacy of the call through nature of the interaction, questions asked, and information requested.

### Key Issues

The extent to which the authentication of the requesting entity required human activity, judgment, and/or person-to-person interaction was identified as a key aspect for this scenario. Work group members pointed out that many of the processes used to authenticate the entity requesting information were not easily translated to rules that allow machine-to-machine interactions between institutions.

When the work group was asked how they authenticate external providers or entities that electronically access health records, a number of issues surfaced. Although the issue of identifying and authenticating external providers and organizations will be more systematically addressed in other portions of the project, the initial discussion shows:

- There are many authentication tools used to authenticate users, such as login ids, passwords, and biometric controls
- Security fobs that have 5-7 digit random numbers transmitted to them every 60 seconds are another authentication tool currently used by some work group members' organizations. When a health care provider needs to access the electronic health record from an external location, they must supply their login id, a password and the correct

random number. While this system provides very good security, work group members were concerned about the number of fobs that a provider would be required to maintain if they needed to access many different systems.

- Another significant issue identified was the process used to credential health care providers that are granted remote access to the electronic health record. The issue is significant for two reasons. First, there are clear variations in how the process is handled. Some organizations accept the provider's credentialing by the other organization being provide remote access. Other organizations require the provider to be credentialed by their process prior to granting access. The second reason this is a significant issue is that credentialing providers is an expensive and time-consuming process.

**Business Practice Variation**

The business practices used to authenticate users and entities in the scenario revealed no significant variation. This lack of variation is not surprising given that the exchange is conducted almost exclusively by telephone and fax. However when the question is expanded to ask how external or remotely-situated providers are authenticated, there are significant variations. These variations include variations in credentialing providers, managing a directory of authorized users, and authentication methods. A number of work group members recommended having a structured discussion of these specific issues independent of a specific scenario.

**Information Authorization and Access Controls**

Variation Work Group members did not identify variations or concerns regarding information authorization and access controls in the scenario, because the exchange was being done person-to-person over the telephone. However, work groups members did express concerns about the difficulty of transitioning human-based interactions to machine-based interactions. Specifically, they expressed concern about the ability to build trust and existing relationships into electronic systems.

As the discussion moved beyond the facts of the scenario into a more general discussion of access controls, one work group member indicated the importance of establishing both behavioral controls and system controls. Many other work group members agreed and indicated that behavioral controls are as important, and perhaps more important than system controls.

Work group members pointed out that in a paper-based world, inappropriately accessing a medical record required a trip to the Medical Records Department and asking another person for the physical record. However as electronic health records are more accessible within an organization, there is an increased risk of inappropriate access or "social surfing." Work group members pointed out that this increased accessibility of health information increases the need to implement behavioral and system controls. However, work group members were also quick to state that previously, it was difficult to know the extent to which medical records were inappropriately accessed. Yet in electronic health records it is much easier to document access and identify inappropriate access.

Another general issue related to access controls was identified as a barrier to exchanging information. One work group member's organization is unable to provide remote access to its electronic health record for physicians treating patients across a clinic and hospital setting when the hospital and clinic are separate organizations. The work group member indicated that the electronic health record system is unable to restrict access to only patients who consented to sharing information with other organization's providers. This indicates that some electronic health record systems need to have additional access controls built into their systems to more fully facilitate the appropriate sharing of health information and implementation of more sophisticated access controls.

**Information Audits that Record and Monitor Activity**

Work group members indicated that there were no significant variations in their recording and documenting the exchange of information in the scenario. Work group members indicated that their organizations all had policies requiring documentation related to providing health information to another hospital or facility. The documentation would include details such as, any paper or documents generated through the exchange (e.g., a faxed request, consent forms, etc.), the requester of the information, documentation of consent to disclose information or the reason consent is not possible, and information disclosed. While there were no variations across organizations, a number of work group members indicated that there may be variations within organizations based on the facts of this scenario. Specifically, if two physicians from the two hospitals were talking over the telephone to exchange the information in an emergency situation, the documentation of the exchange may or may not be documented.

**State Law Restrictions**

Work Group members did not identify any State law restrictions in requesting the information described in the scenario, although they did identify Minnesota’s requirements for patient consent to release health records (see Minnesota Statutes §144.335, Subd. 3a) as a potential restriction.

**Key Issue**

Variation Work Group members stated that, in general, they need to have consent to authorize the disclosure of health information. However, Minnesota law permits a health care provider to release health information for a medical emergency when the provider is unable to obtain the patient’s consent. Thus, most work group members believed that they would be able to legally disclose the information being requested in this scenario.

**Business Practice Variation**

The business practice variation associated with this scenario does not arise from different policies, but rather from organizations exercising judgment and differently balancing patient risk with organizational risk (see also, the discussion of Emergency Treatment in the Impact of Key Issues section).

As described previously, work group members indicated that they would initially request consent authorizing the disclosure of the requested health information. When presented with information that the situation was an emergency and that patient consent would not be possible, most work group members indicated that they would disclose the information. At least one organization indicated that given the facts of this specific scenario that their organization would probably insist on obtaining consent before disclosing the information. Other work group members also indicated that determining when to disclosure of information without consent is very situation specific, and depending on the situation, may require the involvement of the organization’s Health Information Manager or Privacy Officer.

**Legal Issues**

The judgment used in deciding if a situation is a medical emergency and a provider may release health information without the patient’s written consent as provided by Minnesota Statutes § 144.335, Subdivision 3a (b) (1) can be a source of variation when providing health information to another health care provider.

---

## IDENTIFIED BARRIERS OR BEST PRACTICES

---

The only barrier specifically identified within this scenario is the barrier that is created when:

1. The emergency room determines that it really needs the diagnosis and treatment information for the 89-year-old patient;
2. The 89-year-old patient is unable to consent because of her injuries or confusion; and
3. The hospital being asked to disclose the health information determines that the situation is not an emergency that would allow the release of health information under Minnesota Statutes § 144.335, Subdivision 3a (b) (1).

Another barrier indirectly identified through this scenario relates to the general issue of how external or remotely-situated providers are authenticated when trying to access electronic health records. While there are mechanisms and methods to ensure very strong security, many of the mechanisms are not consistent or conducive with needing to access multiple electronic health record systems across a variety of health care organizations. There currently exist significant variations in how organizations approach this issue. These variations can in themselves be a barrier to exchanging health information between health care providers. A number of work group members recommended having a structured discussion of the issues related to user and entity authentication such as, credentialing providers, managing a directory of authorized users, and authentication methods. The work group will devote time at future meetings to address these issues.

## ANALYSIS OF SCENARIO #2 PATIENT CARE - SCENARIO B

---

### SCENARIO OVERVIEW

---

*A specialty substance abuse treatment facility wants to refer client X to a primary care facility for a suspected medical problem. The client has a long history of using various drugs and alcohol relevant for medical diagnosis. The information is being sent to the primary care provider without the patient's authorization. The primary care provider refers the patient to a specialist and sends all of their information (without patient authorization) including the information received from the substance abuse treatment facility to the specialist.*

*NOTE: We realize that Minn. Statutes 144.335 generally requires consent unless the health records are being released to other providers within related health care entities when necessary for the current treatment of the patient. To consider additional issues within this scenario, we'll assume that we get patient consent consistent with Minn. Statutes § 144.335.*

To provide some structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified two key issues and five questions for consideration (see Expanded Scenario #2). The two key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The two key issues identified were:

- **Patient Consent/Authorization:** This issue was identified as a key issue because Minnesota law generally requires patient consent to release health information. Additionally, this scenario calls for the sharing of chemical dependency treatment information, which under Federal regulations requires patient authorization. We assume that health care organizations have a number of policies and procedures related to patient consent/authorization ensuring their organizations' compliance with State and Federal law. Another reason for identifying patient consent as a key issue is that consent is an important mechanism for patients to exercise control over the use and sharing of their health information.
- **Handling of Health Information Regarding Substance Abuse Treatment:** This issue was identified as a key issue because Federal regulations require patient authorization to disclose chemical dependency information. Also, patients are often more concerned about sharing substance abuse treatment information than other health information.

The five questions for consideration were intended to focus the work group's discussion, as well as to provide slight modifications to the scenario. The scenario is very specific and likely to evoke very specific, fact-dependent business processes. In order to have a more complete discussion of the scenario, we introduced small changes to the facts of the scenario in an effort to identify their impact on the business processes related to the exchange of the information. The five questions attempted to:

- Determine if any specific or additional consents are required to share chemical dependency/substance abuse treatment information with other health care providers either inside or outside an organization
- Determine if organizations' electronic health records have special controls to restrict access to substance abuse treatment records

- Assess how organizations use electronic logs to record access and disclosures of substance abuse treatment data
- Investigate if organizations place additional security measures on chemical dependency/ substance abuse treatment data when exchanging the data electronically or on paper
- Describe the intersection of the scenario with the nine privacy and security domains used within the project

---

## **GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO**

---

This scenario surprised most of the Variation Work Group members. A number of the members pointed out that under Federal regulations; it was unclear how a facility could release chemical dependency information without patient consent in a non-emergency situation. Given that the disclosure of the health information in this scenario is generally governed by Federal regulations, Work Group members questioned why there would be variation across states and organizations in the exchange of these data.

### **Exchanging Substance Abuse Treatment Information**

Variations Work Group members were unanimous in stating that the Federal regulations prohibit chemical dependency records to be transferred without the proper patient authorization. All members stated that their organizations require a patient authorization that: a) specifically listed chemical dependency treatment data as information to be disclosed; and b) specifically listed the name of the organization to which the information is to be disclosed. There were no variations between Work Group members' organizations in the release or transfer of substance abuse treatment data.

### **Internal Handling and Use of Substance Abuse Treatment Information**

The Variations Work Group members' discussion revealed significant variation in how substance abuse treatment data is handled and used within different organizations. One hospital restricts access to chemical dependency data to the specific unit within the hospital. The hospital also stated that while a patient was in the chemical dependency unit of the hospital, the patient health record was maintained on paper and the electronic health record was only used for storing chemical dependency records after the course of treatment. In general, the organization's policies restricted access to these records without consent. However, if a patient were transferred from the chemical dependency unit to a medical unit for additional treatment the chemical dependency treatment information would follow the patient without additional consent, but only within their facility and as part of a transfer.

Another organization described their policy that restricts access to chemical dependency records to those providers involved in the patient's chemical dependency treatment. However, this hospital permits providers in their emergency department and urgent care center to access medication data in the chemical dependency records. However in accessing the medication information, health care providers are required to provide a written reason in the electronic health record for accessing the medication information.

A third organization, that uses a centralized electronic health record across a number of organizations, stated that it permits all physicians and facilities sharing the electronic health record to access chemical dependency and behavioral health data as needed to treat the patient. These organizations use an "overall" patient consent stating that the medical staff using the centralized electronic health record can access health information as needed to treat the patient.

These three organizations show that significant differences exist in organizations' internal policies and procedures for accessing and using chemical dependency data. Most of the Work Group members' organizations have some policies or procedures to limit access to chemical dependency information and the

differences between organizations reflect the different responses to patients' sensitivities. Interestingly, despite using a variety of different internal controls and mechanisms, there were few variations related to the disclosure of substance abuse treatment data to outside organizations.

### **Impact of Key Issues**

**Patient Consent/Authorization** policies and procedures are clearly dictated and standardized by the Federal regulations related to the disclosure of chemical dependency treatment data. The Work Group verified that patients are concerned about the disclosure of these data and want to control how the data are disclosed. One work group member stated that patients receiving treatment for chemical dependency and behavioral health request more restrictions on sharing their information than other patients. Many patients do not want this sensitive information shared with anyone, including their own primary care doctor.

**Handling of Health Information Regarding Substance Abuse Treatment** seemed to vary greatly between organizations with different organizations implementing different policies and controls to limit access to only appropriate access. All organizations clearly recognized patients' sensitivities to the use and disclosure of substance abuse treatment and their various policies reflect these sensitivities.

### **Variations in Business Practice**

As stated above, there were many variations in the internal protections applied to substance abuse data, but few variations in the requirements associated with the disclosure or exchange of substance abuse data outside of the organization.

---

## **APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario, including the modifications addressed in the questions for consideration. Recognizing that the exchange contemplated by the scenario occurs almost exclusively by paper, Work Group members were also asked to describe issues that would arise if this exchange were to be conducted electronically between organizations.

### **Information Audits that Record and Monitor Activity**

Variation Work Group members indicated that their organizations generally maintained logs that allowed them to monitor and audit access and activity within electronic health records, including chemical dependency records. Most systems have the capability to log and track all access to the health records, although some systems only log and track edits to records. Hence, there is variation between organizations as a result of the capabilities of their particular information systems.

Logs tracking access to health records generate significant volumes of data. Using electronic logs to proactively monitor appropriate system use is difficult given the volume of information in the log and the number of staff that have appropriate access to health records for treatment, payment and business operations. Consequently, most organizations use a complaint-driven process to investigate concerns about inappropriate access to health records. If there is a concern that a record is being inappropriately accessed, organizations assign staff to investigate the specific complaint. The Work Group estimated that 85% of organizations are doing complaint-based log review. Some organizations also conduct VIP reviews to monitor inappropriate access to the health records of well-known individuals; that is, those individuals most likely to attract attention from "social surfers."

Another consequence of the significant volumes of data generated by logs tracking access to health records is that the logs require substantial amounts of electronic storage space. This is a significant issue because there are multiple logs and multiple information systems. The result is that logs can quickly grow to

unmanageable amounts of information. Trying to manage the amount of data creates another variation between organizations in the length of time that they maintain audit logs. The variation is not only between organizations, but also within organizations as the requirements and value of logs vary between different information systems.

### **Key Issue**

An issue that has been raised by consumers as part of this project is the notion that as health information is stored electronically, it will be possible for patients to obtain a listing of all individuals (e.g., medical staff, billing staff, etc.) who have accessed the patient's health information. Similarly, consumers have suggested that it would be possible to obtain a listing of all external individuals (e.g., other health care providers, health plans, etc.) who have received the patient's health information. In general, Work Group members did not believe this level of accounting for access was practical, or even feasible.

While many organizations log individuals that access particular electronic health records, Work Group members doubted that such logs would be understandable to patients. Many staff members within a hospital legitimately access the health record as part of the treatment provided to the patient. Similarly, many staff members appropriately access the health record for the payment process and business operations (e.g., quality assurance program). Consequently, a patient receiving such a log would not be able to understand why the record was accessed, what information was used, or if the access was appropriate within the organization. This is the primary reason that most organizations currently use a complaint-based review of logs.

Even tracking all disclosures of health information would be problematic. All Work Group members' organizations obtain patient consent prior to routine releases of health records for continuity of care and/or payment. Thus, patients are able to exercise control over the release of their health information. However, organizations do not maintain a log or accounting of the health information released to other providers for continuity of care. Likewise, provider organizations do not maintain a log of the disclosures of health information to payers as part of the payment process. The primary mechanism for protecting patients' privacy is the consent requirement, not the review of audit logs.

A number of provider organizations questioned the value of maintaining or making available a log of all disclosures. They drew an analogy to the accounting for disclosures currently required under the HIPAA Privacy regulations. Currently, most providers are required to account for most disclosures of health information that are done without patient authorization, excluding those disclosures for treatment, payment and operations. However since the regulations effective date in 2003, most provider organizations have had only a handful of patients requesting the accounting for disclosures. Similarly, the Work Group questioned if the number of requests and the limited utility of the data would justify the costs associated with maintaining logs that could be made available to patients. Most Work Group members felt that a complaint-driven system was more realistic and effective.

### **Administrative or Physical Safeguards**

Variation Work Group members indicated that there were no special or unusual safeguards applied to substance abuse treatment data beyond the access controls described in the "Internal Handling and Use of Substance Abuse Treatment Information" sections of this analysis. The primary administrative control associated with the exchange of this type of health information is patient consent. Hence, as long as appropriate patient consent has been obtained, consistent with federal regulations, substance abuse treatment information should be able to be exchanged in a manner consistent with other health information.

**State Law Restrictions**

Work Group members did not believe that Minnesota law was driving the restrictions associated with exchanging substance abuse/chemical dependency information. While Minnesota law generally requires patient consent to release health information, Federal regulations have very specific requirements for patient authorization to disclosure chemical dependency treatment information. One Work Group member remarked that following the Federal chemical dependency restrictions to the letter of the law was a very difficult task. It was suggested that as health care organizations become more connected and information can be exchanged more easily, the health care industry could use greater clarity and input from the Federal regulators on the application of the Federal chemical dependency regulations.

---

**IDENTIFIED BARRIERS OR BEST PRACTICES**

---

The Variations Work Group discussion around this scenario clearly shows that patient consent/authorization is the most important protection/barrier to the exchange of substance abuse treatment information. Work Group members did not describe the Federal chemical dependency regulations as a barrier that needs to be removed. In fact, Work Group members recognized patients' concerns and sensitivities to the sharing this type of data, and their organizations have a number of policies to ensure that consent requirements are satisfied before information is disclosed or exchanged. However, the discussion also demonstrates that as more information is exchanged electronically, it will be necessary to have mechanisms that facilitate satisfying the consent requirements and electronically documenting patient consent within a health information network of connected providers. Work Group members also agreed that Federal regulators should provide further guidance on the application of the chemical dependency laws to increasingly interconnected networks of health care providers sharing health information to treat patients.

## ANALYSIS OF SCENARIO #3 PATIENT CARE – SCENARIO C SECURITY AND ACCESS

---

### SCENARIO OVERVIEW

---

*At 5:30 pm 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. At the time of the patient's transfer, the discharge summary and other pertinent records were electronically transmitted to the 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. Unable to access the long-term care 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 the 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 long-term care facility notifies Dr. X's office that it is unable to open the encrypted document because it does not have the encryption key.*

To provide structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified three key issues and six questions for consideration (see Expanded Scenario #3). The three key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The identified issues were:

- **Provider Authorization and Access to Electronic Health Records:** This issue was identified as a key issue because authorizing a health care provider to view medical information is often the first step in granting access to electronic health records. It was anticipated that organizations have policies and practices to approve and authorize health care providers' access to electronic health records.
- **Exchanging Summaries and Abstracts between Electronic Health Records:** This issue was identified as a key issue because organizations frequently exchange discharge summaries and abstracts. It was anticipated that organizations have policies and practices in place to address these exchanges of information.
- **Transcription Services:** This issue was identified as a key issue because many organizations use external transcription services and electronically exchange information with the services. It was anticipated that organizations have addressed privacy and security issues related to the use of transcription services.

The six questions for consideration were intended to focus the Work Group's discussion and attempted to:

- Determine if and how a physician visiting a facility for the first time would be permitted to access an electronic health record.
- Investigate the processes associated with granting new physicians access to organizations' electronic health records (e.g., credentialing, training, etc.).
- Examine the use of transcription service portals and measures taken to secure data exchanged through these portals.
- Investigate processes for merging data from other information systems (e.g., other facilities or transcription service portals) into organizations' electronic health records.
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

### GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

Many nursing homes are not currently using electronic medical records. One Work Group member estimated the adoption rate at approximately 25%. Additionally, long term care facilities' electronic medical records tend to focus on admission paperwork, Medicare and Medicaid documentation requirements, and medication histories. These electronic medical records do not generally include as much medical information as is typically included in a hospital's electronic health record system. Nursing homes' limited use of electronic health records made certain parts of this scenario difficult to evaluate.

To have a more complete discussion of the scenario, we asked other types of health care providers the same general questions asked of nursing homes. Hospitals and clinics also have policies related to authorizing providers' access to electronic health records, interacting with transcription services, and merging data from external sources into their electronic health records. Therefore, we asked the questions associated with this scenario generically enough so that many different types of health care providers could address them.

#### Providing Health Information to Visiting Physicians

The nursing homes indicated that specialty physicians infrequently visit patients in the nursing home. It is much more common for patients to go to the physician's office. If a physician arrived at a long term care facility to visit a patient for the first time, the facility's front desk would first verify the physician's credentials. The nursing home would require picture identification and some documentation of the individual's credentials as a physician. The physician would then be directed to the charge nurse for the patient's area within the nursing home.

The charge nurse would assist the physician in accessing the health records whether they were maintained on paper, electronically, or some combination of electronic and paper records. This stage of the process would also serve as a secondary check on the physician's credentials because the physician's name and/or his medical facility's name would likely appear on the requested health records. If the requested records are on paper, the charge nurse would locate the appropriate information and the physician would be permitted to review the materials at the charge nurse's desk. If the requested records are part of an electronic system, the charge nurse would login to the system, find the appropriate records, and sit with the physician while the records are reviewed. Having the charge nurse sit with the physician as he reviews the records serves two purposes. First, it is a security measure ensuring that only the appropriate information is accessed. Second, it is a practical measure ensuring that the physician has the ability to navigate the electronic record which may be in an information system which is unfamiliar to the physician.

A number of Work Group members from hospitals and clinics pointed out that there may be another option for the physician to access the information. Assuming that the physician is affiliated with the hospital that supplied the discharge summary, it is very likely the physician would have the ability to remotely access the hospital's electronic health record through a secure internet connection. This remote access would provide the physician access to his patient's health records back at the hospital or clinic facilities.

In contrast to nursing homes, the hospitals and clinics on the Variations Work Group indicated that a visiting physician would not be permitted to practice medicine in their facilities until the physician went through the full medical credentialing process. The credentialing process includes documenting the physician's credentials to practice medicine, providing proof of insurance, investigating any existing complaints/sanctions with appropriate regulatory bodies, and other similar activities. This process is not an immediate one that could be done while the physician waits.

Hospitals and clinics also limit access to their electronic health records until users have been appropriately trained. Most organizations' training addresses applicable policies and practices, privacy and security issues, and use of the electronic health record application. Some organizations also require users to pass a competency test at the end of training. After successfully completing any training and testing requirements, users are provided everything needed to access the electronic health record such as a login ID, passwords, and a security fob.

### **Exchanging Summaries and Use of Transcription Services**

The nursing homes in the Variations Work Group indicated that they are not currently exchanging discharge summaries and physician assessments electronically. Rather, the information is provided to the long term care facilities on paper and is sent to the facilities with the patient, through the US mail, or via fax. The paper records are placed into the patient's paper chart and select items are entered into the nursing home's electronic medical record (e.g., medications).

The nursing homes do not receive physician assessments via e-mail because hospitals and clinics generally prohibit the exchange of patient-identified data via unsecured e-mail. Additionally, many organizations do not support or encourage the use of secure e-mail to exchange patient-identified health data, because the process for securing e-mail is generally considered difficult and cumbersome for end-users to implement. The situation described in this scenario, where encrypted documents could not be opened by the receiving organization, highlights the difficulty in trying to implement secure e-mail. Consequently, most organizations do not generally use e-mail as a mechanism for exchanging patient-identified health information.

Many of the hospitals and clinics in the Variations Work Group indicated that their organizations use transcription services and require the transcription services to sign a business associate agreement as required by the HIPAA Privacy regulations. After executing an appropriate contract, the organizations access transcriptions through a secure portal. Generally, the organizations assign particular staff responsibility for logging into the portal, downloading the transcriptions, and importing the information into the appropriate electronic health records. The Work Group members believed that the use of a transcription service with appropriate contracts in place is no greater privacy concern than the normal privacy concerns associated with employees. It was also noted that a number of organizations were working toward the ability to dictate directly into their electronic health record system. There are a number of advantages to direct entry including greater privacy and security when fewer people need to exchange and handle patient data.

### **Impact of Key Issues**

**Provider Authorization and Access to Electronic Health Records:** A physician visiting a nursing home for the first time would be required to show identification and credentials to gain access to patient data. Generally, the nursing home patient's information would be in a paper medical record, which the charge nurse would provide to the physician. If the patient's information is available in an electronic medical record, the charge nurse would access the record and guide the physician through the record.

Hospital and clinics require visiting physicians to be medically credentialed prior to practicing medicine in their facilities. Additionally, these organizations require individuals who access their electronic health records to go through training that addresses privacy, security, and application-specific training.

**Exchanging Summaries and Abstracts between Electronic Health Records:** Hospital discharge summaries and other related information is currently exchanged with long term care facilities on paper and is sent with the patient, through the US mail, and via fax. Most organizations either prohibit or strongly discourage the transmission of patient-identified data through e-mail because of the difficulties of appropriately implementing security measures.

**Transcription Services:** Work Group members that use transcription services require a business associate agreement to be included in the contracting process. Information from a transcription service is then downloaded through a secure portal by employees responsible for importing the information into the appropriate portions of the organization's electronic health records.

### **Variations in Business Practice**

There were very few variations between similar types of health care entities, although there were differences between entities from different areas of the health care industry. For example, nursing homes allow visiting physicians to access patients' medical records by showing identification and credentials. In contrast, hospitals and clinics require physicians to be medically credentialed prior to practicing in their facility or accessing the electronic health records. At long term care facilities, charge nurses may assist visiting physicians in accessing needed information in medical records (usually on paper), whereas hospitals and clinics require users of their electronic health records to attend some type of training prior to being permitted access to the organization's electronic health record.

---

## **APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario. No additional issues were identified.

---

## **IDENTIFIED BARRIERS OR BEST PRACTICES**

---

One of the most significant barriers to the electronic exchange of health information with nursing homes is the limited degree to which most nursing homes have implemented electronic health records capable of interacting with other information systems. However, this barrier is not a privacy and security barrier, but rather a fiscal and technological constraint.

The most significant privacy and security barrier to the electronic exchange of health information is the limited support of secure e-mail. Many organizations prohibit or strongly discourage the transmission of patient-identified health information via e-mail. Some organizations have no mechanism for securing such e-mails and therefore directly prohibit the transmission of patient-identified data. Other organizations have the ability to secure the e-mail, but the process is cumbersome and may not always be utilized by end users. These organizations therefore discourage the transmission of patient-identified data to minimize the risk of sending improperly secured e-mails.

## ANALYSIS OF SCENARIO #4 PATIENT CARE - SCENARIO D

---

### SCENARIO OVERVIEW

---

*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 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 because other family members have had breast cancer.*

To provide some structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified four key issues and four questions for consideration (see Expanded Scenario #4). The four key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The four key issues identified were:

- **Patient Consent:** This issue was identified as a key issue because Minnesota law generally requires patient consent to release health information. We assume that health care organizations have a number of policies and procedures related to patient consent ensuring their organizations' compliance with State law. Another reason for identifying patient consent as a key issue is that consent is an important mechanism for patients to exercise control over the use and sharing of their health information.
- **HIV-related Health Information:** This issue was identified as a key issue to identify any Minnesota laws that might restrict the disclosure or exchange of HIV-related health information differently than other health information. We also anticipated that patients might be more concerned about sharing HIV-related health information than other health information, and we wanted to determine if organizations had instituted additional restrictions for sharing this health information.
- **Genetic Health Information:** This issue was identified as a key issue because the 2006 Minnesota Legislature passed a new law restricting the collection, storage, use, and disclosure of genetic health information. We also anticipated that patients might be more concerned about sharing genetic health information than other health information, and we wanted to determine if organizations had instituted additional restrictions for sharing this health information.
- **Exchange of Digital Images:** This issue was identified as a key issue because many organizations have implemented picture archive and communication systems (PACS) to store, use and link digital images to electronic health records (EHR). Because many organizations have substantial capacity to store and use digital images internally, we anticipated that there might be some advanced capacity to exchange this type of health information electronically.

The four questions for consideration were intended to focus the Work Group's discussion, as well as to provide slight modifications to the scenario. The scenario is very specific and likely to evoke very specific, fact-dependent business processes. In order to have a more complete discussion of the scenario, we introduced small changes to the facts of the scenario in an effort to identify their impact on the business processes related to the exchange of the information.

The four questions attempted to:

- Determine if any special or additional consents are required to share/disclose HIV-related health information
- Assess if organizations have specific policies or controls that limit or monitor access to HIV-related health information in their electronic health records in ways that are different than the policies and controls for other health information
- Determine if any special or additional consents are required to share/disclose genetic health information
- Assess if organizations have specific policies or controls that limit or monitor access to genetic health information in their electronic health records in ways that are different than the policies and controls for other health information
- Investigate the capacity to electronically exchange digital images and identify privacy/security issues associated with such exchanges
- Describe the intersection of the scenario with the nine privacy and security domains used within the project

---

### **GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO**

---

In the analysis of other scenarios within this project, it was noted that a health care provider/organization can always request another provider to supply a patient's health information. However, the responsibility for ensuring that any exchange of health information is appropriate and consistent with legal requirements resides with the health care provider supplying or disclosing the information. Consequently in analyzing this scenario, we consistently asked the Variations Work Group members to place themselves in the position of the organization being asked to exchange or disclose the health information.

#### **Exchanging/Disclosing HIV-Related Health Information**

Part of this scenario envisions the exchange of Patient X's health records, which would contain HIV-related health information. The Variations Work Group was asked if their organizations had specific policies or consent requirements associated with disclosing HIV-related health information. In general, the policies related to the exchange of HIV-related health information differed only slightly from the policies for the exchange of other health information.

Under Minnesota law, patient consent is required to release patient health records to another provider in non-emergency situations. Minnesota law does not have additional patient consent requirements to release HIV-related health information. Consequently, many organizations do not treat HIV-related information differently than any other health information. Some organizations provide check boxes on patient consent forms that permit patients to specifically opt-in or opt-out of consenting to disclose HIV-related health information. These check boxes are not required under law, but serve as a mechanism to eliminate confusion and misunderstandings between the provider and the patient. The check boxes allow patients to make more informed decisions by reminding them of sensitive information that may be in their health record. Many times patients are only thinking about the health information related to their most recent visit and not about all of the information in their health record. The most significant difference between organizations is one organization requires the patient consent to specifically reference HIV-related health information in order for their organization to disclose the information.

All organizations use the same general mechanism for protecting privacy – patient consent. The primary difference between the organizations is the ease with which a patient can choose to restrict HIV-related health information. Beyond differences in the consent forms, HIV-related health information is treated the same as any other health information and does not receive special handling.

### **Exchanging/Disclosing Genetic Health Information**

Part of this scenario envisions Patient X having genetic testing for breast cancer genes. The Variations Work Group was asked if their organizations had any specific policies or consent requirements associated with disclosing this health information to another health care provider. All Work Group members said that their organizations had no specific policies or consent requirements associated with disclosing genetic health information. This information was treated exactly the same as any other health information.

The Variation Work Group was asked if they had been able to assess the impact of a new law (Minnesota Statutes § 13.386) passed by the 2006 Minnesota Legislature restricting the collection, storage, use, and disclosure of genetic health information. Because the law was recently passed, organizations had not yet analyzed its impact or implemented the requirements into their activities. Although the requirements of the law have not yet been implemented, we anticipate that it will effect health care organizations in the near future.

### **Exchanging/Disclosing Digital Images**

Part of this scenario envisions exchanging digital images of Patient X's previous mammogram. The Variations Work Group was asked if their organizations would be able to electronically exchange the digital images. Most organizations indicated that they generally shared digital images with other organizations by: a) printing the image on film; or b) by putting the image on a CD-ROM along with an applet (i.e., software program) that allows the image to be viewed. The organizations indicated that exchanging images through a CD-ROM and applet was better than trying to directly exchange digital images, because one of the difficulties of trying to exchange digital images is that other providers' PACS may not be able to read an image and allow it to be viewed.

The usual process for exchanging digital images is to first obtain the patient's consent to disclose the information. Next, the digital image is put onto a CD-ROM along with the applet. Finally, the CD-ROM is then sent to another health care organization by providing the CD-ROM to the patient or by courier. When asked about any security measures placed on the CD-ROM, Work Group members responded that the images usually had no security measures (e.g., password protected or encrypted).

One organization that frequently works with other health care providers in the rural area pointed out that the bandwidth of internet connections presented another barrier to exchanging the digital images through direct connections. Digital images are often very large computer files and a high-speed internet connection is required to ensure adequate bandwidth to exchange the files.

### **Impact of Key Issues**

**Patient Consent:** The Variations Work Group members were unanimous in stating they would require patient consent to share any of the patient information in this scenario with other health care providers. Except for one organization that required HIV-related information be specifically listed in the patient consent, all of the organizations used the usual consent processes that are used to disclose other health information.

**HIV-related Health Information:** There are no special state requirements related to the exchange of HIV-related health information. However, a number of organizations recognize patients concerns about this information by providing check boxes on their consent form allowing patients to easily opt-in or opt-out of sharing HIV-related information with other providers.

**Genetic Health Information:** Currently, the process for exchanging genetic information is identical to the process for exchanging other health information. The 2006 Minnesota Legislature passed a new law that places requirements on organizations' collection, storage, use, and disclosure of genetic health information. However, organizations have not yet incorporated this law into their policies and practices.

**Exchange of Digital Images:** Currently, digital images are not exchanged through direct electronic interchange, but rather, on CD-ROM or film. The most significant barriers to direct electronic interchange of digital images are:

1. Compatibility between different organizations' PACS (e.g., DICOM standards, implementation versions, etc.); and
2. Inadequate bandwidth in rural organizations' internet connections

**Variations in Business Practice**

The discussion of this scenario did not reveal significant variations in the business policies and practices. All organizations obtained patient consent prior to exchanging or disclosing the health information described in this scenario. The Work Group described minor variations in the consent forms used for the disclosure of HIV-related information with some organizations providing check boxes that allow patients to easily opt-in or opt-out of sharing the information. Also, one organization requires HIV-related information be specifically listed in the patient consent to release HIV-related information.

The processes used for exchanging digital images also showed little variation with most images exchanged on CD-ROM with an applet or on film. While the current process for exchanging digital images was consistent, the lack of consistent technical standards across organizations' PACS was identified as a significant variation that creates a barrier to direct electronic interchange of digital images.

---

**APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario, including the modifications addressed in the questions for consideration. Recognizing that the exchange contemplated by the scenario occurs almost exclusively by paper for health information and via CD-ROM and film for images, Work Group members were asked to describe issues that would arise if this exchange were to be conducted electronically between organizations.

**Patient and Provider Identification**

One Work Group member described the difficulty of patient identification that can occur when digital images are exchanged on CD-ROM. Often digital images are exchanged between organizations as part of a radiological consult. When the image is sent on a CD-ROM, it may contain only the most basic demographic information about the patient (e.g., name). The radiologists would like to be able to index the image and link it to other images stored in the PACS for the same patient. However when the patient has a common name that matches many other patients' name, there may be no way to properly and uniquely link the image to the appropriate patient. Similarly, there may no way to uniquely link the image to the appropriate patient record in the electronic health record

Organizations have procedures to address this patient identification issue and verify the identity of patient in the image. However, the verification process necessary to index the digital image into the PACS system is time consuming and organizations do not have sufficient resources to ensure that every image is indexed, stored in the PACS, and linked to the patient's electronic health record. Consequently, radiologists may need to provide a consult based solely on the image supplied and without comparing it to other images.

Depending on the reason for the radiological consult, patient identification can be a significant issue. If the image is a broken bone, the ability to link to other images and the electronic health record may not be a significant problem. However if the image is a lung nodule, it is very important to be able to link images and compare current and older images. Organizations use their verification processes and resources to collect the data necessary to index and link images in the most important and significant situations in order to not compromise patient safety. However, overall patient safety could be improved and fewer resources expended if there was better patient identification and demographic information exchanged with digital images.

**Information Transmission Security or Exchange Protocols**

Although most organizations do not exchange digital images through direct electronic interchange, they often allow their radiologists to access digital images from remote locations through high-speed internet connections. Some organizations also contract with outside radiologists to provide services for their facility and need to exchange digital images with the contract radiologists. In both of these situations, the transmissions are secured through the use of a virtual private networks (VPNs) that exchange encrypted data between the remote locations and an organization's PACS.

**Administrative or Physical Safeguards**

The Variations Work Group's discussion of administrative safeguards focused primarily on policies and practices related to the use of e-mail. Many organizations have adopted a policy that patients' health information will not be included in e-mail messages unless the e-mail is secure e-mail (e.g., encrypted). The implementation of this policy has created two issues.

The first issue arises when a health care organization receives data or test results that indicate a problem (e.g., mammogram that shows potential cancer). Organizations want to provide the information quickly to the appropriate treatment provider; however, they also want to alert the patient as quickly as possible as well, so that the patient can start to take action. One way to alert the patient would be through e-mail, but this is generally not possible because it is very difficult to send secure e-mails to patients.

The second issue arises from the way certain providers typically conduct their work. For example, pathologists frequently e-mail each other to discuss and consult about test results. It is important to provide secure e-mail to providers that routinely consult with other providers through e-mail. Thus, work group members strongly encouraged other organizations to examine how all of their providers may be using e-mail to conduct their work and to provide secure e-mail solutions to facilitate that work.

**State Law Restrictions**

Work Group members did not identify Minnesota laws that affected the exchange of health information in this scenario beyond Minnesota's usual patient consent requirements. It was noted that Minnesota has a new (effective August 2006) genetics law requiring informed patient consent for the collection, storage, use, and disclosure of genetic information. Variations Work Group members' organizations have not yet had the opportunity to incorporate the requirements of the new law into their policies and procedures. The law is expected to significantly impact the use and disclosure of genetic information through the requirements described below in Minnesota Statutes § 13.386, Subdivision 3:

Subd. 3. **Collection, storage, use, and dissemination of genetic information.**

Unless otherwise expressly provided by law, genetic information about an individual:

- (1) may be collected by a government entity, as defined in section 13.02, subdivision 7a, or any other person only with the written informed consent of the individual;
- (2) may be used only for purposes to which the individual has given written informed consent;

(3) may be stored only for a period of time to which the individual has given written informed consent; and

(4) may be disseminated only:

(i) with the individual's written informed consent; or

(ii) if necessary in order to accomplish purposes described by clause (2). A consent to disseminate genetic information under item (i) must be signed and dated. Unless otherwise provided by law, such a consent is valid for one year or for a lesser period specified in the consent.

---

### IDENTIFIED BARRIERS OR BEST PRACTICES

---

The discussion of this scenario identified a few issues that could currently be considered barriers to the electronic exchange of digital images. The first barrier to the exchange of digital images is that different organizations' PACS may use different technical standards (e.g., DICOMM standards) for storing and viewing digital images. Although not a privacy/security issue, the variance in standards makes direct interchange of digital images difficult. The current solution to this barrier is to exchange the digital images via CD-ROM and include an applet that allows the image to be viewed.

The second barrier to the direct interchange of digital images is the bandwidth required to exchange large computer files like most digital images. This problem is more acute in rural areas where health care providers may not have access to high-speed internet connections. Again this barrier is not a privacy/security issue, but the lack of adequate bandwidth for rural providers makes direct interchange of digital images difficult.

The third issue identified with the exchange of digital images is the potential difficulty of correctly identifying the patient associated with the image. When digital images are exchanged between health care providers on CD-ROM, there may not be sufficient patient identifying information and demographic information to properly index/link the image to the patient's other images in the PACS or to the patient's electronic health record. While organizations have verification procedures to address this problem, it is a time-consuming and resource-intensive process. Unlike the other two issues, this problem is a privacy/security issue within the context of this project. Also unlike the other two barriers to the exchange of digital images, this issue is not a barrier to direct interchange, but rather, a barrier to the ability to fully use digital images exchanged today CD-ROM.

While health care organizations have many common and similar policies to protect the privacy and security of their patients' health information, one practice stood out as a potential best practice. Many organizations have a policy that patients' health information will only be exchanged via secure e-mail. Because secure e-mail between organizations can be difficult to implement, many organizations have a policy that they do not send information outside their organization via e-mail. However, some providers (e.g., pathologists) routinely communicate with each other via e-mail to discuss test results. Thus, Work Group members strongly encouraged organizations to examine all providers' compliance with their e-mail policy and to consider the use of secure e-mail for providers who frequently use e-mail as a tool for their work process.

## ANALYSIS OF SCENARIO #5 PAYMENT SCENARIO

---

### SCENARIO OVERVIEW

---

*X Health Payer (third party, workers compensation, 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 by its case management staff to approve/authorize inpatient encounters.*

To provide some structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified three key issues and five questions for consideration (see Expanded Scenario #5). The three key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The three key issues identified were:

- **Use of Health Information for Payment versus Treatment:** This issue was identified as a key issue because patients often have more concerns about sharing health information for activities other than treatment, including payment. Also, we anticipated that providers may have different policies related to providing access to health information for treatment than for payment.
- **Payer Access to Electronic Health Records:** This issue was identified as a key issue because it was anticipated that it would be a particularly sensitive issue for both patients and health care providers. Patients are concerned about payers and insurance companies having access to their health information through an EHR, because they are concerned that the payer will use the data for inappropriate activities (e.g., underwriting or raising premiums). Providers have various concerns, including that payers will use the information unfairly in negotiating payment rates.
- **Access to Electronic Health Records by Outside Entities:** This issue was identified as a key issue because health care providers are concerned about the security risks associated with permitting outside providers and organizations access to their information systems. We expected that health care providers have specific policies and procedures related to providing outside entities access to their electronic health records or other systems.

The questions for consideration were intended to focus the Work Group's discussion, as well as to provide slight modifications to the scenario. The scenario is very specific and likely to evoke very specific, fact-dependent business processes. In order to have a more complete discussion of the scenario, we introduced small changes to the facts of the scenario in an effort to identify their impact on the business processes related to the exchange of information.

The questions attempted to:

- Determine whether provider organizations would consider a payer’s request to access the electronic health record for case management to be access for treatment or payment purposes
- Identify concerns that health care providers would have with health plans accessing their organization’s electronic health record
- Investigate if and how health care providers currently send electronic health information to payers’ case management staff to approve/authorize inpatient encounters
- Identify health care providers’ privacy and security concerns when allowing outside entities (e.g., providers or others) access to their electronic health record
- Describe the intersection of the scenario with the nine privacy and security domains used within the project

---

## **GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO**

---

### **Granting Health Plans/Payers Access to Electronic Health Records**

Health care providers participating in the Variations Work Group stated that none of their organizations currently permit health plans to access their electronic health records. Furthermore, most indicated that they would never let health plans have remote access into their electronic health record.

The providers did not feel that the health plans’ case management activity was an appropriate activity for direct access to their organization’s electronic health record. Most providers have clinical management staff that work with health plans on issues such as case management. The provider organization’s staff has access to the health information necessary to satisfy the health plans’ case management informational needs. The necessary information is exchanged between the providers and payers via telephone, fax, and web portal. Most provider organizations believe that the current methods of exchanging information are more appropriate than providing access through their electronic health records because:

1. It allows the health care provider greater control and ability to limit the exchange of information to the minimum necessary information as required under the HIPAA Privacy regulations;
2. It reduces the security risks associated with granting outside entities access to the electronic health record and ensuring that the data are only used for appropriate purposes; and
3. It eliminates any worries that payers would use a provider’s information for inappropriate uses.

Health care providers identified at least one situation where they permit health plans to access their electronic health record. When health plans want to perform chart audits, providers will often permit the health plan to access the electronic health record. However, the access is usually done from a cube within the health care provider’s location and under the supervision of the health care provider’s staff. Health care providers also have the ability to monitor and track the records and information reviewed as part of the chart audits.

### **Providing Health Information for Pre-Authorization**

As stated in the previous section, most health information exchanged between health care providers and health plans for case management or pre-authorization is exchanged over the telephone, via fax or through a web portal. The Work Group was asked if there would be a reason to create a “payer portal” or “pre-

authorization abstract” that provided health plans limited access to the electronic health record for only the information necessary to authorization a patient’s encounter. The Variations Work Group questioned both the need and value of a payer portal or pre-authorization abstract.

Some Work Group members questioned the need for a standardized “payer portal” or “pre-authorization abstract” by pointing out that under HIPAA, the ANSI X12N 278 Health Care Services Review Information Transaction is already a “standard transaction” for conducting patient pre-authorizations. Although most organizations are incapable of conducting the X12N 278 transaction, the Work Group questioned the need to create another transaction for the same function.

Work Group members also questioned the value of trying to create a standardized “payer portal” or “pre-authorization abstract.” The Work Group was concerned that any savings acquired by reducing billing staff costs would be more than consumed in additional information systems staff costs. Additionally, there were concerns that the “standard” for the abstract would not really be standard and that different payers would continue to have different requirements that changed on a regular basis. One work group member summed up the situation by saying, “We already have a standard that doesn’t work. We do not need another one that doesn’t work.”

### **Impact of Key Issues**

**Use of Health Information for Payment versus Treatment:** Most Variations Work Group members treated case management requests in this scenario as either health care operations or payment activities. Most members felt that the distinction was not relevant to the discussion, because Minnesota law requires patient consent for the health information to be exchanged between the provider and health plan regardless of its classification.

**Payer Access to Electronic Health Records:** Health care providers do not currently provide health plans access to their electronic health records. Additionally, health care providers have little interest in providing health plans access to their electronic health records in future. Health plans are only granted access to a health care providers’ electronic health record for very specific purposes (e.g., chart audits), and then only at the provider’s physical location and under the provider’s supervision.

**Access to Electronic Health Records by Outside Entities:** Health care providers are very concerned about the security risks associated with allowing access to their electronic health record to outside entities of any kind. Even allowing other health care providers access to the electronic health record for patient treatment raises concerns. Regardless of the administrative policies and contractual assurances put into place, it is difficult for providers to be comfortable with the organizational risks that come from permitting access to electronic health records.

### **Variations in Business Practice**

There were not significant variations in the business policies and practices used by Variations Work Group members in terms of the key issues of this scenario, namely:

1. Providers do not currently give health plans access to their electronic health records for payment activities;
2. Providers do not want to give health plans access to their electronic health records for payment activities in the future;
3. The exchange of case management and pre-authorization information is being done through telephone, fax, and web portals; and
4. Providers are very concerned with the organizational risks associated with allowing any outside entity access to their electronic health record, regardless of the appropriateness of that access.

While there were not variations in the general business policies and practices, Work Group members did identify variations in health plans' informational requirements for pre-authorization. These variations serve as a barrier to simplifying the exchange of that information. Currently, most providers and health plans exchange health information for pre-authorization over the telephone, via fax, or through a web portal and the information that needs to be submitted can vary greatly between payers. As stated earlier, the HIPAA administrative transactions have a standard for the electronic exchange of pre-authorization information, although the standard has done little to normalize the data exchanged. A number of Work Group members criticized the current situation with comments such as:

- "HIPAA has given us standards without real standards."
- "Administrative simplification would be great...if we really had it."
- "Even implementation guides don't have all the answers."

Health care providers were pessimistic that providing Payers access to their EHR would make this process any more time efficient or cost effective.

---

## APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario, including the modifications addressed in the questions for consideration. Recognizing that the exchange contemplated by the scenario occurs almost exclusively by telephone, fax and web portal, work group members were asked to describe issues that would arise if this exchange were to be conducted electronically between organizations.

### **Information Audits That Record and Monitor Activity**

A couple of Work Group members addressed the way their organizations accommodate outside organizations that need access to their electronic health records for chart audits (e.g., HEDIS auditors, research grant auditors, compliance auditors, etc.). The organizations generally ask for a list of records or criteria for records that the auditor would like to view. Some organizations use the list to create a restricted view within their system that is limited to the listed records, thus prohibiting the auditor from inappropriately accessing other records. Other organizations allow the auditor more direct access to the electronic health record, but maintain a log of the records accessed by the auditor. The log is then reviewed immediately after the auditor completes the chart review to verify that no inappropriate records were accessed. In all cases, the chart audits are done at the health care provider's location and under the supervision of the health care provider's staff.

### **State Law Restrictions**

Minnesota Statute § 144.335 requires patient consent for health care providers to release health information to health plans for the claim payment related activities, such as pre-authorization. In addition, The Minnesota Insurance Fair Information Reporting Act (Minnesota Statutes § 72A.49-.505) place restrictions and requirements on insurers' collection, use, and disclosure of health information.

Although Minnesota Statutes have multiple requirements for patient consent, there was a question about the quality of the protections provided by those requirements. Work Group members noted that patients are often given a significant number of consents, authorizations, and other paper work when visiting a health care provider. Frequently there is insufficient time to read all of the materials and patients may or may not understand what they are signing. Health care organizations have only modest resources (staff and time) to address questions about the consent materials. In addition, patients are often sick and worrying about their

physical health instead of their health information. Consequently, Work Group members wondered whether patients really understood how much of their health information may be shared with a payer after they sign the patient authorization forms.

---

### IDENTIFIED BARRIERS OR BEST PRACTICES

---

The greatest barrier to the information exchange contemplated by this scenario is not a problem of privacy and security, but rather one of inadequate standards. The providers in the Variation Work Group rejected the notion that payers need access to their electronic health records for pre-authorization activities. The Work Group noted that HIPAA provides a standard transaction in the ANSI X12N 278 Health Care Services Review Information Transaction. However, to date most organizations are incapable of conducting the X12N 278 transaction and the data elements required varies across payers. Making the existing transaction truly standard and functional would provide a better mechanism for exchanging pre-authorization information than providing health plans remote access to electronic health records.

One general barrier to electronic exchange of health information is the perceived liability facing organizations for allowing inappropriate access to information. Variation Work Group members are very concerned about allowing outside entities access to their electronic health records. The concern is often expressed in terms of "organizational risk" or liability. The organizations are concerned about potential data breaches, inappropriate access, accidental disclosures, and the ability to properly protect their patients' data. One consequence of these worries is that organizations are very cautious in connecting to outside organizations and allowing access to patients' health information. Many organizational policies and procedures for sharing patient data are greatly influenced by organizations' attempts to balance improved patient safety with reduced organizational risk.

## ANALYSIS OF SCENARIO #7 RESEARCH DATA USE

---

### SCENARIO OVERVIEW

---

*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 project is being reviewed by the IRB that presides over research protocols at the major medical center where the research investigators are located. The data being collected are all electronic and all responses from the subjects are completed electronically in the same data base file.*

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

To provide structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified three key issues and seven questions for consideration (see Expanded Scenario #7). The three key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The identified issues were:

- **Use of Health Information for Research:** This issue was identified as a key issue because patients often have concerns about using identifiable health information for activities other than treatment such as research. Also, we anticipated that organizations have specific policies related to the use of health information for research activities.
- **Expansion of Research beyond Existing Institutional Review Board (IRB) Approvals and Research Protocols:** This issue was identified as a key issue because IRBs exist to assure that the rights and welfare of the human subject are protected. When research activities expand beyond approved research protocols, research subjects can be harmed, including through the loss of privacy. Consequently, we anticipate that organizations conducting research have clear and unambiguous policies related to the use of IRBs and modifying research protocols.
- **Exchange of Research Data across State Lines:** This issue was identified as a key issue because the Minnesota e-Health Advisory Committee asked us to investigate if patient consent requirements in Minnesota Statutes § 144.335, Subd.(d) created problems exchanging health information for research, particularly with other states.

The seven questions for consideration were intended to focus the Work Group's discussion and attempted to:

- Investigate how organizations doing research record and store research subjects' health information in electronic health records and/or separate databases.
- Explore if organizations engaged in collaborative research allow external researchers remote access into their electronic health records or other data systems.
- Determine organizations' policies related to expanding data collection and data use beyond the IRB-approved research protocols.

- Assess organizations' policies and safeguards to limit access and use of individually identifiable health information for research to appropriate access and use.
- Determine if organizations have any difficulties disclosing or exchanging research data with researchers in other institutions or states.
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

### **GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO**

---

The Variations Work Group was asked to discuss their business policies and practices for using individually identifiable health information for research. In doing so, they identified research as being a more significant issue for their organizations than many other internal uses of data. Some of the research-related issues they face include:

- Distinguishing between research and quality assurance, which is classified as a health care operation.
- The expansion or modification of research activity beyond the research protocols approved by their Institutional Review Board.
- Students with access to health information for treatment purposes who use their access to patient data to collect data for their theses without obtaining the necessary approvals.
- Limiting researchers' access to patient identifiable data to the minimum necessary for the research project.

Given the many different stakeholders represented on the Variations Work Group, the types of research conducted varied greatly. Some organizations conducted no research. Some organizations performed health services research through retrospective use of medical record data or administrative claims data. Other organizations participated in all forms of research including large-scale clinical trials. The variety of research conducted by different organizations tended to influence their policies and view of research; however, the organizations shared many similar policies.

#### **Definition of Research Versus Quality Assessment**

The HIPAA Privacy regulations define research as:

*a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.*

The HIPAA Privacy regulations also include the following activities as health care operations:

*Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.*

While quality assessment and research activities may be very similar, the difference between the activities is very important for organizations. All of the Variations Work Group members' organizations conduct a variety

of quality assessment activities that are classified as health care operations. These activities are subject to the organizations' usual policies concerning the use of health information for health care operations. Organizations that conduct research have additional policies and requirements intended to ensure research activities do not compromise patients' privacy.

The transition between quality assessment and research is an important and sometimes difficult issue for organizations. In the course of conducting quality assessment activities, an organization may find an interesting result and want to publish the finding in a scientific journal. This evolution from quality assessment to research requires staff to comply with the organization's research policies (e.g., obtaining IRB approval). For organizations it is not easy to know when a project has changed from quality assessment to research and thus know that it needs to enforce its research policies. Hence, the organizations are keen to help staff/researchers appreciate when the switch has occurred and the importance of complying with research policies.

### **Research Protocols Reviewed by an Institutional Review Board**

All Variations Work Group members' organizations that conduct research using individually identifiable health information use an Institutional Review Board (IRB) to ensure compliance with Federal requirements for the protection of human subjects, as well as the HIPAA Privacy regulations.

This scenario calls for two uses of patient-identifiable data that appear to be outside of the IRB-approved research protocols:

1. Investigators would like to use the raw data to track the patients over an additional six months; and
2. An investigator would like to use the raw data collected for a white paper that is not part of the research protocol's final document for his post doctoral fellow program.

For both of these situations, Variation Work Group members were unanimous in stating that their organizations would require the investigators to have these changes to the research protocols evaluated by an IRB. The Work Group acknowledged that it is not unusual for students to want to go beyond approved research protocols and use data for their theses, and the organizations are diligent in helping these researchers understand and follow IRB policies.

### **Use of De-Identified Data**

This scenario involved a clinical trial, which is always subject to an IRB review. However, much of the research conducted by health care providers and health plans is health services research that uses existing data sources (e.g., medical charts, administrative claims). Much of this research can be done using de-identified data as defined under the HIPAA Privacy regulations. Because the use of de-identified data for research does not jeopardize a patient's rights or welfare, de-identified data does not require an IRB to approve the research. Consequently, Variations Work Group members' organizations make every effort to conduct research using de-identified data. Many organizations create data warehouses or data sets of de-identified data to facilitate their researchers' use of data.

### **Use of Individually Identifiable Health Information**

When Variations Work Group members' organizations conduct research using individually identifiable health information, they require the research to be reviewed by an Institutional Review Board. After the IRB review and approval, researchers may begin data collection process, which may be:

- Primary data collection of patient data in a clinical trial as described in this scenario; or

- Secondary data extraction from existing data sources such as an electronic health records system or administrative claims database.

The data collection process is important because it has implications for how the data are stored and accessed.

### **Primary Data Collection, Storage and Use**

When data are collected directly from the patient in a clinical trial, the medical information relevant to the patient's treatment is stored and maintained in the patient's electronic health record. That medical information in the electronic health record is available to the other providers involved in the patient's treatment. If the research protocol called for collecting additional non-medical information from the patient, that data would be stored outside of the electronic health record in a secure database.

While providers/researchers access and use the electronic health record to treat the patient, the analyses of patients' data are done in a separate, secure database. Organizations extract the appropriate data from the electronic health records and create a separate, secure database for the research project. It is from this database that researchers conduct the research project's statistical analyses. Creating the separate database is done for a number of reasons, including:

1. It limits the access of non-providers involved in the research project, to only the data needed for the research project; and
2. It helps avoid delays in response time in the electronic health record system by ensuring that research projects are not unnecessarily using resources.

### **Secondary Data Extraction, Storage and Use**

When the research project uses secondary data from existing sources, Variations Work Group members' organizations have some formal process for researchers to request the data. The process is designed to ensure that the data requester has complied with the appropriate organizational requirements, such as IRB review and approval. Once the data requester has documented that they have complied with the relevant requirements, the data are extracted and provided to the research team in an appropriate format (e.g., database, view of a database, etc). All statistical analyses are conducted using this extracted data set.

Limiting access to individually identifiable patient data, whether in an electronic health record or in a data warehouse, and using a formal process for requesting data is a cost-effective control to ensure that data are not used inappropriately.

### **Exchanging Data with External Researchers**

Minnesota Statutes § 144.335, Subd.(d) places requirements on healthcare providers who release/disclose health records to external researchers. While the HIPAA Privacy regulations generally require patient authorization, the regulations also permit IRBs to waive or alter patient authorization requirements. In situations where research is conducted without patient authorization, Minnesota's statutory requirements are relevant. Specifically, the following requirements would apply:

- *health records generated before January 1, 1997, may be released if the patient has not objected or does not elect to object after that date;*
- *for health records generated on or after January 1, 1997, the provider must:*
  - *disclose in writing to patients currently being treated by the provider that health records, regardless of when generated, may be released and that the patient may object, in which case the records will not be released; and*

- o *use reasonable efforts to obtain the patient's written general authorization that describes the release of records in item (i), which does not expire but may be revoked or limited in writing at any time by the patient or the patient's authorized representative.*

While many organizations obtain the patient's written general authorization as part of their usual consent process, the Statute also provides a mechanism for establishing authorization:

*authorization may be established if an authorization is mailed at least two times to the patient's last known address with a postage prepaid return envelope and a conspicuous notice that the patient's medical records may be released if the patient does not object, and at least 60 days have expired since the second notice was sent; and the provider must advise the patient of the rights specified in clause (4);*

The impact of these statutory requirements has diminished over time. HIPAA generally requires patient authorization for the use of individually identifiable health information to be used for research and this authorization satisfies Minnesota's requirements. Many organizations have been obtaining this general authorization as part of their normal business practice, so they are meeting the requirements. The Minnesota requirements seem to primarily affect those organizations whose usual consent processes do not include the patient's general authorization to release health records to a researcher. However, it is only a barrier to the exchange of health information with an external researcher when the health information identifies patients and an IRB has provided a waiver or altered the need for patient authorization.

**Impact of Key Issues**

**Use of health information for research:** Many Variations Work Group members' organizations use health information for research. These organizations want to make certain that the research activities do not jeopardize their patients' privacy. Consequently, the organizations make every effort to conduct research using de-identified data. When research requires the use of patient identifiable data, the research protocols are reviewed by an IRB. Access to data for research is generally restricted, and organizations use a formal process for granting access to the data. This process allows the organizations to ensure that appropriate policies have been followed (e.g., IRB review, minimum necessary).

**Expansion of Research beyond Existing Institutional Review Board (IRB) Approvals and Research Protocols:** All Variations Work Group members' organizations that conduct research using individually identifiable health information use an Institutional Review Board. All of the organizations have policies and practices that restrict access and use of identifiable data for research without appropriate IRB review and approval. Similarly, all of the organizations require that changes to research protocols be re-reviewed by an IRB, regardless of the reason for a change in protocol.

**Exchange of Research Data across State Lines:** While Minnesota Statutes § 144.335, Subd. (d) imposes conditions for the exchange of individually identifiable health information for research activities, it was not identified as a significant barrier. As organizations have adapted their business practices to comply with the HIPAA Privacy regulations and to accommodate Minnesota's statutory requirements, the impact of the requirements has diminished. There were no specific issues or barriers identified for inter-state exchanges of individually identified health information.

**Variations in Business Practice**

Work Group members identified minor variations in the type of research conducted by their organizations, the consent forms used for patient authorization, and the details of getting access to data for research. However, the Work Group members did not identify variation in the most significant aspects of this scenario. That is, there are not variations between organizations regarding:

- Their policies to limit data used for research to the minimum necessary and to use de-identified data whenever possible;
- Their policies requiring compliance with research-related requirements under the HIPAA Privacy regulations and Minnesota Statutes 144.335, Subd.(d).;
- Their policies that require research conducted with patient identifiable data to be reviewed and approved by an IRB;
- Their policies that all changes to IRB approved research protocols must be re-reviewed by an IRB;
- Their policies to limit access to patient data until data requests can be appropriately reviewed; and
- Their policies requiring that data analysis be done in a separate and secure database, rather than from within an electronic health record system.

---

### **APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario.

#### **Information Audits That Record and Monitor Activity**

For some federally funded research, the funding agency will require an audit of researchers' original data sources. When the research collects medical information and stores it in electronic health records, this means that auditors need access to the electronic health records. Work Group members' organizations accommodate auditors by asking for a list of records that the auditor would like to view. Some organizations create a restricted view within their system, limited to the listed records, thus prohibiting the auditor from inappropriately accessing other records. Other organizations allow the auditor more direct access to the electronic health record, but maintain a log of the records accessed by the auditor. The log is reviewed immediately after the auditor completes the chart review verifying that no inappropriate records were accessed. In all cases, the chart audits are conducted at the health care provider's location and under the supervision of the health care provider's staff.

---

### **IDENTIFIED BARRIERS OR BEST PRACTICES**

---

The HIPAA Privacy regulations, 45 CFR Part 46 Protection of Human Subjects, and Minnesota Statutes § 144.335 all contain requirements that must be met for the use of individually identified health information to be used in research. These requirements all serve as valuable controls to help ensure and protect patients' privacy. Work Group members identified the protections as requirements that have been incorporated into their business policies and practices, but they did not identify the protections as barriers that need to be eliminated.

## ANALYSIS OF SCENARIO #8 ACCESS BY LAW ENFORCEMENT

---

### SCENARIO OVERVIEW

---

*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 arrives in the ER in addition to the patient's parents. 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 are made to the ER staff.*

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

To provide structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified three key issues and four questions for consideration (see Expanded Scenario #8). The three key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The identified issues were:

- **Health Information Given to Law Enforcement:** This issue was identified as a key issue, because it was anticipated that law enforcement requesting information is a frequent occurrence. Releasing health information to law enforcement is a significant issue for patients, and health care organizations undoubtedly have policies and processes addressing law enforcement's access to patient information. Other than mandated reporting (e.g., gunshot wounds), we believe that Minnesota law does not allow health care providers to release health information to law enforcement except through a warrant or court order.
- **Health Information Given to Insurance Subscribers:** This issue was identified as a key issue in order to determine what health information would be made available to insurance subscribers regarding other people insured under the same insurance policy. It was also included to clarify how health information may be disclosed inadvertently through the explanation of benefits (EOB) sent by payers after an episode of care covered under insurance.
- **Health Information Given to Parents:** This issue was identified as a key issue in order to determine how a health care organization's response to a parent's request for health information about their child may vary with the age of the child.

The four questions for consideration were intended to focus the work group's discussion, as well as to provide slight modifications to the scenario. The scenario is very specific and likely to evoke very specific, fact-dependent business processes. In order to have a more complete discussion of the scenario, we introduced small changes to the facts of the scenario in an effort to identify their impact on the business processes related to the exchange of the information. The four questions attempted to:

- Investigate any differences in the privacy rights of adults and minors for drug and alcohol treatment data
- Determine the rights of insurance subscribers to view the health care information of other individuals covered under the same policy and to investigate the practical ability to limit the disclosure of information that may be included in the explanation of benefits

- Determine the rights and requirements of law enforcement to access patients' health care information
- Describe the intersection of the scenario with the nine privacy and security domains used within the project

---

## GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

### Providing Information

The Variations Work Group was asked to identify the business policies and processes used when their organization is asked to disclose health information to law enforcement, insurance subscribers or parents. In general, work group members stated that disclosure of the health information described in the scenario requires either the patient's consent or a warrant or a court order. The Variations Work Group members were unanimous in stating that law enforcement would only be granted their request for patient health information if: a) the patient consented; or 2) law enforcement produced a warrant or court order.

The Variations Work Group members were also unanimous in stating that they would not disclose health information to the insurance subscriber (e.g., parents) without the patient's consent. However, the members did point out that some health information may inadvertently disclosed as part of the payer's explanation of benefits statement (EOB) sent to the patient as part of the payment process. While processes related to send EOBs to patients is outside the control of health care providers, many providers advise patients that the inadvertent disclosure of information may be prevented by: a) the patient paying for the service out of their pocket; or b) specifically requesting that the insurance company to send the EOB to a different address and to not share the health information.

Finally, the Variation Work Group members stated that a 19-year old child's health information would only be shared with the parents with the consent of the 19-year child.

### Impact of Key Issues

**Health Information Given to Law Enforcement:** Law Enforcement's access to health information was unambiguous. The Variations Work Group was unanimous in stating that law enforcement would be denied access to the patient's health record unless a court order or warrant was produced. Work group members had ambivalent feelings regarding police and law enforcement in their emergency departments. On the one hand, emergency departments are grateful that the police are around the emergency departments to provide security. On the other hand, the problem of having the police "hanging around" the emergency department creates concerns about accidental or incidental disclosure of health information and requires careful management so records and computer screens are not compromised.

The Variation Work Group members all agreed that their organizations faced a constant challenge regarding education and training on privacy and security issues related to law enforcement and health information. The internal emergency department staff plus ancillary groups like transportation need to periodically review privacy policies and procedures and remember that even if law enforcement officers asked friendly, seemingly innocuous questions, the privacy rights of the patients needed to be diligently honored.

Likewise, health care organizations need to work with their law enforcement partners to educate and remind them of the legal restrictions and requirements associated with disclosing patient health information to law enforcement.

**Health Information Given to Insurance Subscribers:** The Variation Work Group members were unanimous in stating that when confronted with the request of health information by the insurance

subscriber, in this case the parent, they would automatically deny the request unless directed to do otherwise by the patient. It was noted that the parents might be inadvertently receive health information when the insurer send an explanation of benefits statement (EOB) for the event.

**Health Information Given to Parents:** As stated above, the Variation Work Group members were unanimous in stating that when confronted with the request of health information by the parent, they would automatically deny the request unless directed to do otherwise by the patient.

Work group members also referenced Minnesota Statutes § 144.335 and 144.343 which, in combination allow any minor to give effective consent for medical, mental and other health services to determine the presence of or to treat pregnancy and conditions associated therewith, venereal disease, alcohol and other drug abuse. Given that the health information referenced in this scenario is drug and alcohol related, parents would not be allowed access to the health information for any child 13 years of age or older. However, if the patient were under 13-years of age, the parents would be granted access.

### **Variations in Business Practice**

There are no significant variations in the business policies and practices used by Variations Work Group members related to the disclosure of the health information described in this scenario. The lack of variation among health care organizations in responding to this scenario is not surprising. Minnesota Statutes (§144.335) explicitly require patient consent in disclosing health information. Work group members' organizations have implemented these requirements into their policies and processes.

The only variation identified during the discussion was attitudinal variation related to how organizations viewed law enforcements continual presence in the emergency department. Some providers saw law enforcement omnipresence as a potential nuisance and a distraction requiring additional security and privacy safeguards; other providers welcomed law enforcement as an additional component of their physical security.

---

## **APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario, including the modifications addressed in the questions for consideration.

### **Information audits that record and monitor the activity**

Work group members indicated that there were no significant variations in their recording and documenting the exchange of information in the scenario. Work group members indicated that their organizations all had policies requiring documentation related to providing health information to law enforcement and others.

### **Administrative or physical safeguards**

Work group members indicated that there were times when the police would be in and around emergency department and that parents might be with the patient; therefore, care needed to be taken so that computer screens and charts were not visible or accessible to those seeking inappropriate access. The work group did not discuss the specific administrative and physical safeguards that were used to address these types of inappropriate disclosures. The particular types of policies and practices used needs to be further addressed in a general discussion of this domain.

### **State Law Restrictions**

Work Group members identified Minnesota Statutes § 144.335 and 144.343 as restrictions in providing the health information described in the scenario and its variations. Specifically, work group members'

organizations require the patient's consent, a warrant, or a court order for the disclosures described. Variation Work Group members all seemed to interpret the law the same way and have the same general procedures.

---

### IDENTIFIED BARRIERS OR BEST PRACTICES

---

There really were no barriers specifically identified within this scenario because each organization interpreted the relevant laws exactly the same way and there seemed to be great unanimity in policies and procedures to address this scenario. Even when the scenario was expanded to include four questions about various aspects of the health care organizations policies and procedures no significant barriers emerged to prevent the electronic exchange of health information.

## ANALYSIS OF SCENARIO #9 PHARMACY BENEFIT - SCENARIO A

---

### SCENARIO OVERVIEW

---

*The Pharmacy Benefit Manager (PBM) has a mail order pharmacy and also has a closed formulary. The PBM receives a prescription from Patient X 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.*

To provide structure for the Variations Work Group members' discussion and analysis of this scenario, staff identified one key issue and six questions for consideration (see Expanded Scenario #9). The key issue identified was the aspect of the scenario that was anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between Work Group members. The identified issue was:

- **ePrescribing:** This issue was identified as a key issue because it was anticipated that health care providers are increasingly considering mechanisms and processes to electronically exchange prescription data with pharmacies. As organizations evaluate adding the capacity to electronically exchange these data, they need to address privacy and security issues.

The six questions for consideration were intended to focus the work group's discussion and attempted to:

- Investigate current mechanisms for exchanging drug prescription data.
- Determine if prescription data is exchanged electronically.
- Investigate the processes for exchanging information when a pharmacy determines that a prescribed drug is not on a patient's formulary.
- Assess the barriers to increased electronic exchange of prescription data.
- Explore the linkages, if any, between health care providers' electronic health records and health plan formularies.
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

### GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

#### **Exchanging Prescription Drug Data**

Variations Work Group members identified four ways that drug prescription data are exchanged between health care providers and pharmacies:

1. The prescription is "auto-faxed" from the electronic health record to the patient's pharmacy;

2. The prescription is printed out of the electronic health record, signed by a physician, and manually faxed to the patient's pharmacy;
3. The patient is provided a written prescription, either from an electronic health record or prescription pad, and the patient takes it to the pharmacy directly; and
4. The health care provider exchanges the prescription with the pharmacy over the telephone.

Within the Work Group, the most common mechanism for exchanging prescription data was options 1 and 2 – faxing the data. In a typical situation, the health care provider enters the drug prescription into the electronic health record and asks the patient which pharmacy they would like to fill the prescription. The information is then automatically faxed to the appropriate pharmacy directly from the electronic health record. When the information is auto-faxed, the electronic health record signs the prescription using an electronic signature that is stored in the system.

When the drug being prescribed is a Schedule II drug, pharmacies will not accept an auto-fax. The prescription must be printed, signed by a physician, and manually faxed to the pharmacy. These requirements are done to discourage inappropriate drug seeking, and not as a patient privacy/security protection.

Some pharmacies will accept a prescription over the telephone, particularly in rural areas. However, pharmacies are increasingly refusing to accept prescriptions over the telephone and require that the information be faxed. The faxed prescription provides the pharmacy with a written record of health care providers' exact prescription. This method of exchange eliminates opportunities for the pharmacy to incorrectly document the information through transposition of numbers, mishearing dosages, and other transcription errors.

The Work Group members did identify variations in how pharmacies accept information. Some pharmacies, including large national chains, will only accept a fax (manual or auto-fax). Other pharmacies, particularly mail order pharmacies, are unwilling to accept an auto-fax and want a manual fax. Some small pharmacies are unable to accept a fax and require the information to be exchanged over the telephone.

Once the prescription has been faxed to the pharmacy, the information is manually transferred to the pharmacy's information system. No Work Group member reported having the ability to electronically exchange prescription information directly from an electronic health record to a pharmacy's information system. Interestingly, the Work Group members representing large integrated health care systems with hospitals, clinics and pharmacies report using the same general processes. That is, the information is faxed internally to the integrated system's pharmacy and the information is manually entered into the pharmacy's information system. The key difference between the integrated systems' pharmacies and external pharmacies is that integrated systems' pharmacists have access to their organization's electronic health record and can access records to identify allergies or other medications that could counter-indicate the drug being prescribed.

#### **Addressing Formulary Issues**

When filling prescriptions, pharmacies will check the patient's insurance benefits and occasionally discover that the prescribed drug is not included in the health plan's formulary. Pharmacies then telephone or fax the health care provider to notify them that the prescribed drug is not consistent with the patient's formulary. After being alerted to the formulary issue, health care providers respond in one of two ways:

1. They generate a letter stating that the patient needs to take the exact drug prescribed. This letter is then faxed back to the pharmacy; or

2. They cancel the previous prescription and issue a new prescription that substitutes a drug included in the formulary for the original drug. The changed prescription is then communicated to the pharmacy via telephone or fax.

The Work Group discussion noted that the time required to resolve a formulary issue can vary from a short period of time to as much as 72 hours. The exact amount of time depends on many factors, such as the type of drug, whether the pharmacy is internal to an integrated system or a mail order pharmacy, provider and pharmacy schedules, and other issues.

### **Linking Electronic Health Records to Health Plan Formularies**

No Work Group member reported having the ability to link their electronic health records to health plan formularies to determine if particular prescriptions are consistent with a patient's required formulary. However, some Variations Group members are investigating software that incorporates such functionality into their electronic health records. One of the difficulties in implementing this type of technology is the large number of formularies that are used by insurers and self-funded health plans. Work Group members indicated that it may not be possible to link with all formularies. However by linking to the largest and most common formularies, the providers would be able to be 95% confident that prescriptions are consistent with patients' required formularies.

### **Impact of Key Issues**

**ePrescribing:** No Variations Work Group members reported having the ability to electronically exchange prescription data from their electronic health record to a pharmacy's information systems. The most common exchange mechanism is faxing the information either manually or directly from the electronic health record. When prescriptions are not consistent with patients' formularies, pharmacies will notify the prescribing provider of the inconsistency via telephone or fax. Health care providers respond back to the pharmacy by telephone or fax with a new, modified prescription or a letter saying the original prescribed drug is required. No Work Group member reported having the ability to link their electronic health records to health plan formularies.

### **Variations in Business Practice**

The Work Group did not identify privacy or security barriers to the exchange of prescription data, although there are significant variations in the policies and practices for exchanging prescription data between health care providers and pharmacies. While the most common mechanisms for exchange are telephone and fax, there are still variations that include:

- Some prescriptions are auto-faxed with electronic signatures and other prescriptions are required to be manually faxed with a manual signature (e.g., Schedule II drugs);
- Some pharmacies require prescriptions to be faxed and refuse to accept prescriptions by telephone, other pharmacies accept both faxed and telephoned prescriptions, and a small number of pharmacies are incapable of accepting faxes; and
- When a prescription is not consistent with a patient's required formulary, the pharmacy and provider exchange information through a mix of telephone and fax communications.

It should be noted that these variations are not generally the result of privacy and security and security concerns, but rather reflect:

- Differences in providers and pharmacies technological capacities;
- Diversity in how organizations manage their operations and workflow;

- The lack of unique standards and protocols (either paper or electronic) for exchanging prescription data; and
- Measures employed to accurately exchange information, avoid transcription errors, and document providers' exact prescriptions.

---

## APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario.

### **State Law Restrictions**

Although not a restriction, the Work Group pointed out that Minnesota Statutes § 151.21 details the conditions under which a pharmacist may substitute a generically equivalent drug for the prescribed drug. Specifically, Subdivision 3 of the section states:

*When a pharmacist receives a written prescription on which the prescriber has not personally written in handwriting "dispense as written" or "D.A.W.," or an oral prescription in which the prescriber has not expressly indicated that the prescription is to be dispensed as communicated, and there is available in the pharmacist's stock a less expensive generically equivalent drug that, in the pharmacist's professional judgment, is safely interchangeable with the prescribed drug, then the pharmacist shall, after disclosing the substitution to the purchaser, dispense the generic drug, unless the purchaser objects. A pharmacist may also substitute pursuant to the oral instructions of the prescriber. A pharmacist may not substitute a generically equivalent drug product unless, in the pharmacist's professional judgment, the substituted drug is therapeutically equivalent and interchangeable to the prescribed drug. A pharmacist shall notify the purchaser if the pharmacist is dispensing a drug other than the brand name drug prescribed.*

This law is not a privacy or security barrier to the electronic exchange of prescription data, although it can influence how pharmacists respond to situations where a patient's prescription is not consistent with a required formulary.

---

## IDENTIFIED BARRIERS OR BEST PRACTICES

---

The Variations Work Group did not identify any privacy or security barriers in exchanging prescription data between providers and pharmacies. Rather the variations and barriers associated with this scenario reflect differences in providers' and pharmacies' technological capabilities, internal workflow decisions, and a general lack of unique standards and protocols for exchanging the information.

## ANALYSIS OF SCENARIO #10 PHARMACY BENEFIT - SCENARIO B

---

### SCENARIO OVERVIEW

---

*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.*

To provide structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified two key issues and five questions for consideration (see Expanded Scenario #10). The two key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The identified issues were:

- **Limited Data Sets, De-Identified Data, and Minimum Necessary Data:** This issue was identified as a key issue because limiting an organization's uses and disclosures of health information to the minimum necessary data for non-treatment activities is a critical privacy protection. In addition, the HIPAA Privacy regulations generally require organizations to limit uses and disclosures of data for non-treatment activities to the minimum necessary data. We anticipated that organizations have policies and practices to limit their disclosures of identifiable health information to the minimum necessary data, especially through limited and de-identified data sets.
- **Secure data exchange:** This issue was identified as a key issue because patients and organizations are growing increasingly concerned about the security and confidentiality of data, particularly when exchanged electronically. We anticipated that organizations have specific policies to address security concerns when electronically exchanging data.

The five questions for consideration were intended to focus the work group's discussion and attempted to:

- Determine if health plans exchange claims data for the activity described in the scenario.
- Investigate if organizations limit the exchange to the minimum necessary data and do so through limited data set or de-identified data.
- Assess if any patient authorization/consent requirements would need to be satisfied to exchange identified data.
- Investigate how data are exchanged and any security measures employed to protect the data.
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

## GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

### Exchanging Claims Data with a PBM

Variations Work Group members that serve as third party administrators (TPAs) for self-insured health plans stated that it is not unusual to request, or be asked for, claims data in order to provide quotes for new business. The TPAs said that they only request or disclose the minimum necessary data needed to provide a quote and that the activities of this scenario can almost always be accomplished with de-identified data.

One of the key activities for this task is the need to match patients' medication histories with their claims data. This linking allows a PBM to evaluate drug usage by diagnosis or underlying condition. The HIPAA Privacy regulations permit entities to assign a code to patient records that allows data linking on the condition that the code is not translatable and otherwise derived from patients' data. Consequently, there is no need to exchange patient-identified data even to link patient records within this scenario.

At least one Work Group member's organization requires the PBM receiving the de-identified data to sign a confidentiality agreement that limits the use of the data, restricts additional disclosures of the data, and addresses other privacy/security issues to protect all subjects of the data (e.g., Company A, health care providers identified in the claims, etc.).

### Method for Exchanging Data

The usual method for exchanging claims data for the purposes of this scenario is on a CD-ROM. Although the data being exchanged is de-identified, the CD-ROMs are always encrypted. Encryption is not necessary to protect the patients' confidentiality, although it provides a second layer of protection to the already de-identified data. Rather, the security measures on the CD-ROM are intended to protect the confidentiality of the other subjects of the data.

One Work Group member indicated that their organization exchanges the information through a secure VPN (virtual private network) connection when the exchange involves extremely large volumes of data.

### Impact of Key Issues

**Limited Data Sets, De-Identified Data, and Minimum Necessary Data:** All Work Group members that serve as TPAs limit the data disclosures required by this scenario to the minimum necessary data, which in this case are de-identified data. Records can be linked within the data set through a non-translatable code for each individual in the record set. At least one organization requires a confidentiality agreement to limit the uses of the data and to protect the confidentiality of all subjects of the data.

**Secure data exchange:** All data exchanged are secured either by encrypting a CD-ROM or through the use of a VPN.

### Variations in Business Practice

There were no significant variations in the business policies and practices used by Variations Work Group members for exchanging de-identified claims data with PBMs to provide price quotes. All organizations apply minimum necessary requirements, use de-identified data in all but rare circumstances, and exchange data via encrypted CD-ROM or other secure method.

## APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario.

### State Law Restrictions

The activities of this scenario can be accomplished with de-identified data, however the Work Group pointed out that their analysis of the situation would change if patient-identified data were required. Minnesota Statutes § 144.335, Subd. 3a requires a patient's written consent to release health records and that consent expires within one year. However, paragraph (c) of the subdivision states:

- (c) *Notwithstanding paragraph (a), if a patient explicitly gives informed consent to the release of health records for the purposes and pursuant to the restrictions in clauses (1) and (2), the consent does not expire after one year for:*
  - (1) *the release of health records to a provider who is being advised or consulted with in connection with the current treatment of the patient;*
  - (2) *the release of health records to an accident and health insurer, health service plan corporation, health maintenance organization, or third-party **administrator for purposes of payment of claims, fraud investigation, or quality of care review and studies, provided that:***
    - (i) *the use or release of the records complies with sections 72A.49 to 72A.505;*
    - (ii) ***further use or release of the records in individually identifiable form to a person other than the patient without the patient's consent is prohibited;***  
*and*
    - (iii) *the recipient establishes adequate safeguards to protect the records from unauthorized disclosure, including a procedure for removal or destruction of information that identifies the patient.*

Additionally, the Minnesota Insurance Fair Information Reporting Act (Minnesota Statutes § 72A.49 through 72A.505) includes TPAs in the definition of insurer and generally requires patient authorization to disclose data. Specifically, Minnesota Statutes § 72A.502, Subd. 1 states:

*An insurer, insurance agent, or insurance-support organization **must not disclose any personal or privileged information** about a person collected or received in connection with an insurance transaction **without the written authorization of that person except as authorized by this section.** [...]*

Minnesota Statutes § 72A.502 does not explicitly authorize the disclosure of patient-identified data for the purposes of this scenario without patient authorization. Therefore, Minnesota law would seemingly require a TPA to obtain patient consent/authorization to release patient-identified data for the purposes of this scenario.

However, the Work Group stated that there is ambiguity about the exact application of Minnesota law to TPAs stemming from the Employee Retirement Income Security Act of 1974 (ERISA) and its preemption of state laws related to employee plans. In general, ERISA preempts state laws that impact or reference an ERISA plan's benefits, structure, or administration. Therefore to the extent that state requirements (e.g., patient authorization) on TPAs may impact the administration of an ERISA plan, the requirements may be preempted. The limits and boundaries of ERISA's preemption are not clear and have been the subject of numerous court cases.

The uncertainty in the relationship between ERISA and state privacy/security requirements is a problem when a self-insured company believes there is a legitimate need to use or disclose patient-identified data from its TPA, which conflicts with state requirements on TPAs. The size and impact of the problem caused by this ambiguity is unknown because it was not the scenario's primary focus. However, this is an issue that the Work Group believes needs to be clarified.

---

### IDENTIFIED BARRIERS OR BEST PRACTICES

---

The Work Group did not identify any barriers to exchanging information for the purposes described in this scenario. However, the Work Group's discussion of this scenario revealed that the relationship between ERISA and state privacy/security requirements should be clarified. That is, there needs to be more detailed guidance on how ERISA's preemption of state laws impacts a state's privacy/security requirements on TPAs administering self-funded health plans.

## ANALYSIS OF SCENARIO #11 HEALTHCARE OPERATIONS AND MARKETING - SCENARIO A

---

### SCENARIO OVERVIEW

---

*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 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.*

To provide structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified two key issues and three questions for consideration (see Expanded Scenario #11). The two key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The identified issues were:

- **Access to Electronic Health Records for Healthcare Operations:** This issue was identified as a key issue because patients often have concerns about using identifiable health information for activities other than treatment, including some types of healthcare operations. Also, we anticipated that providers have different policies for health care operations than for treatment.
- **Minimum Necessary Use and Disclosure of Health Information:** This issue was identified as a key issue because limiting an organization's uses and disclosures of health information to the minimum necessary data for non-treatment activities is a critical privacy protection. In addition, the HIPAA Privacy regulations generally require organizations to limit uses and disclosures of data for non-treatment activities to the minimum necessary data. Hence, we anticipated that organizations have policies and practices to limit their uses of identifiable health information to the minimum necessary data.

The three questions for consideration were intended to focus the Work Group's discussions and to:

- Assess how Work Group members would characterize the requests for health information between healthcare operations and marketing.

- Determine the access and administrative controls organizations employ to appropriately limit use of the electronic health record for healthcare operations such as business planning and conducting cost management
- Ensure that the access and use of health information is limited to the minimum necessary data
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

## GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

The Variations Work Group considered Scenario #11 immediately after considering Scenario #12. In general, the group agreed that the two scenarios were virtually identical in key issues, particularly issues related to the use of individually identifiable health information for health care operations. Given the similarity between Scenarios #11 and #12, the Variations Work Group spent very little time discussing Scenario #11 and considered their review of Scenario #12 as sufficient to address most of the issues in Scenario #11. The only issue that the Work Group singled out for added discussion was the use of minimum necessary data.

### Using Individually Identifiable Health Information for Health Care Operations

Both of the uses of data described in this scenario were determined to be health care operations by the Work Group. As in Scenario #12, organizations do not generally provide direct access to electronic health records for conducting health care operations. Rather, organizations described having a formal process for staff to request the necessary identifiable health information and demographic information. The process requires the requester to specify in detail what data are needed and how the data will be used. The request process allows the organizations to determine the type of activity (e.g., operations, fund raising, etc.), the applicable policies, if the minimum necessary data are being requested, and general appropriateness of the request. If the request for data is granted, the information will be provided to the requester in an appropriate format and media.

The Work Group stressed that any use of identifiable health information for health care operations must limit its use of data to the minimum necessary data. The differences in the minimum necessary data for the two health care operations of this scenario highlights why organizations require data requesters to detail what data are needed and how the data would be used. The Work Group believed that the six-sigma team would be able to have diagnosis and treatment information to conduct cost-planning and other business operations. However, the Work Group questioned the need for any data elements, which could easily be used to identify the patient (e.g., name, address, etc.). Thus, the data provided to the six-sigma team should make it difficult to directly identify patients, although the data would not be de-identified data as defined by the HIPAA Privacy regulations.

In contrast, the Work Group rejected the Marketing Department's need for diagnosis and treatment information in order to send out an informational brochure about the rehab center. In this case, the Marketing Department would be provided with only enough information to mail the brochure, that is, name and address.

### Limiting Use of Health Information

All Variations Work Group members' organizations have policies to restrict non-treatment uses of individually identifiable health information to the minimum necessary. The policy may be applied in one of two ways for health care operations. For routine health care operations, organizations will often create standard reports that limit the data to the minimum necessary. For non-routine health care operations, the organizations

require staff to request data. In reviewing the data request, the organizations explicitly evaluate whether or not the request meets the minimum necessary data requirements.

**Impact of Key Issues**

**Access to Electronic Health Records for Healthcare Operations:** In general, most organizations do not provide access to electronic health records for health care operations, especially the health care operations described in this scenario. The organizations have well defined processes for reviewing data requests for health care operations to ensure appropriateness and compliance with regulatory requirements (e.g., minimum necessary).

**Minimum Necessary Use and Disclosure of Health Information:** Consistent with the HIPAA Privacy regulations, all Work Group members’ organizations have policies and practices limiting the use of individually identifiable health information for health care operations to the minimum necessary data. All data requests are evaluated individually to ensure that requests comply with the minimum necessary requirement and that patient identifiers are removed as much as possible.

**Variations in Business Practice**

There are not significant variations in the business policies and practices for using individually identifiable health information for health care operations. Likewise, there are not significant variations between the Work Group members’ organizations in their application of the HIPAA Privacy regulation’s minimum necessary data requirements.

---

**APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

Variation Work Group members were asked to consider the intersection between the project’s nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario. No additional issues were raised.

---

**IDENTIFIED BARRIERS OR BEST PRACTICES**

---

No data are disclosed or exchanged within this scenario. Consequently, the Work Group did not identify barriers or best practices for the exchange of health information. However, the Work Group discussion pointed out the value of having a formal process for requesting identifiable health information and demographic information, which requires the requester to specify in detail what data are needed and how the data will be used. This process is a critical link in ensuring that the organizations’ policies on minimum necessary data are satisfied and serves as a cost-effective control on inappropriate uses of health data.

## ANALYSIS OF SCENARIO #12 HEALTHCARE OPERATIONS AND MARKETING - SCENARIO B

---

### SCENARIO OVERVIEW

---

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

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

- 1. To provide information on the hospital's new pediatric wing/services.*
- 2. To solicit registration for the hospital's parenting classes.*
- 3. To request donations for construction of the proposed neonatal intensive care unit.*
- 4. They will sell the data to a local diaper company.*

To provide structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified four key issues and seven questions for consideration (see Expanded Scenario #12). The four key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The identified issues were:

- **Access to Electronic Health Records for Healthcare Operations:** This issue was identified as a key issue because patients often have concerns about using identifiable health information for activities other than treatment, including some types of healthcare operations. Also, we anticipated that providers have different policies for health care operations than for treatment.
- **Use of Health Information for Fundraising:** This issue was identified as a key issue because patients often have concerns about using identifiable health information for activities other than treatment, especially activities like fundraising. Also, we anticipated that providers have different policies for fundraising than for treatment.
- **Use of Health Information for Marketing:** This issue was identified as a key issue because patients often have concerns about using identifiable health information for activities other than treatment, especially activities like marketing. Also, we anticipated that providers have different policies for marketing than for treatment.
- **Exchange of Birth Information:** This issue was identified as a key issue because a birth initiates the exchange of health information. The information is exchanged for vital records, newborn screening, and to initiate services for at-risk adults and children. Although this scenario was not explicitly about the exchange of birth-related information, we expanded the scenario to introduce health information exchange into the scenario.

The seven questions for consideration were intended to focus the Work Group's discussion, as well as to modify the scenario. The scenario primarily addresses internal uses of data and not the disclosures of health information. In order to have a more complete discussion of the scenario, we introduced the exchange of birth-related health information to identify its impact on organizations business processes.

The questions attempted to:

- Assess how Work Group members would characterize the Marketing Department’s requests for health information between healthcare operations, fundraising, and marketing.
- Determine the access and administrative controls organizations employ to appropriately limit use of the electronic health record for healthcare operations.
- Investigate organizations’ policies for using data from electronic health records for fundraising.
- Examine organizations’ policies for using data from electronic health records for marketing activities.
- Assess the administrative and physical safeguards organizations employ to ensure that health information is not inappropriately used for health care operations, fundraising or marketing.
- Investigate issues organizations face in electronically exchanging birth information, specifically:
  - Barriers to integrating required reporting requirements (e.g., vital records reporting) into their electronic health records.
  - The capacity of information systems for two-way information exchanges; that is, the ability to send and receive information related to newborns (e.g., services for at risk children or parents, newborn screening results, immunization data, etc.).
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

**GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO**

---

While this scenario described the request for health information as originating from the Marketing Department, Work Group members did not describe all four of the activities as marketing. The first two activities were unanimously considered health care operations. The third activity was judged to be fundraising, and the fourth activity was classified as marketing (see Table 1).

**Table 1: Categorized Uses of Health Information**

<b>Activity</b>	<b>Category</b>
Providing information on the hospital's new pediatric wing/services.	Healthcare Operations
Soliciting registration for the hospital's parenting classes.	Healthcare Operations
Requesting donations for construction of the proposed neonatal intensive care unit.	Fundraising
Selling the data to a local diaper company.	Marketing

These distinctions are important because all of the Work Group members’ organizations have different policies and practices for the different uses of the data.

**Using Individually Identifiable Health Information for Health Care Operations**

The term “health care operations” as defined by the HIPAA Privacy regulations covers a vast set of activities. The discussion of this scenario was not intended to cover every possible use of health information for health

care operations. However, most Work Group members stated that their organizations do not provide individuals with direct access to electronic health records for health care operations, especially the health care operations described in this scenario. Rather, organizations generally use a process for requesting data to be extracted from electronic health records and then given to the individual conducting the health care operations.

Most organizations described having similar processes for making identifiable health information and demographic information available for the internal health care operations described in this scenario. The organizations generally have a formal process for requesting the necessary identifiable health information and demographic information. The process requires the requester to specify in detail what data are needed and how the data will be used. The request process allows the organizations to determine the type of activity (e.g., operations, fundraising, etc.), the applicable policies, if the minimum necessary data are being requested, and general appropriateness of the request. If the request for data is granted, the information will be provided to the requester on an appropriate media, such as a spreadsheet or mailing labels.

A difference between using individually identifiable health information for health care operations and for fundraising was noted during the discussion. In the scenario, the data requester was asking for a targeted population of patients, that is, mothers' demographics for all live births. The use of targeted demographic information is permitted for approved uses such as the health care operations of this scenario. The use of targeted demographic information is not permitted for fundraising activities.

Although the processes making health information available for the internal health care operations were similar across organizations, there are minor variations in the methods used to document and track patients' interest in receiving communications like those described in the scenario. One organization provides patients the opportunity to opt out of such communications as part of its normal consent processes. The organization's consent forms have check boxes allowing patients to indicate if they would like to receive communications about: a) operations; b) treatment alternatives; c) health-related benefits; and d) fundraising. The form also contains a telephone number allowing patients who change their minds to call and opt out of future communications. Most other organizations simply track patients' requests to opt out of future communications as the requests are received. The location for documenting the opt-out requests varies widely across organizations with some organizations documenting the opt-out requests centrally in their electronic health records and other organizations documenting the requests locally in information systems related to the communications.

#### **Using Individually Identifiable Health Information for Fundraising**

The use of identifiable health information and demographic information for internal fundraising had similarities to the use of such data for health care operations, but with some key differences. The most notable similarity was the careful and deliberate process of reviewing the requests for data to conduct fundraising. The process for requesting data is very similar to the process described in requesting data for health care operations. Likewise, any data requests for fundraising are carefully scrutinized to ensure their appropriateness and compliance with relevant regulations (e.g., HIPAA Privacy regulations).

The most notable difference is that some organizations do not conduct fundraising activities and have not used their data for such activities. Another difference is that organizations do not permit using individually identifiable health information to target specific patient populations for fundraising. Hence, requesting birth mothers' demographic information to solicit donations for the construction of a neonatal intensive care unit would be prohibited by all of the Work Group members' organizations.

#### **Using Individually Identifiable Health Information for Marketing**

All Work Group members stated emphatically that their organizations would never use individually identifiable health information for marketing. Any such use of health information would require a patient authorization under the HIPAA Privacy Regulations. Additionally, Minnesota law would require patient consent under

Minnesota Statutes §144.335, Subdivision 3a for the disclosure of the health information for marketing as described in this scenario.

The use of health information for marketing as described in this scenario is so outside the community norm for appropriate use of health information, many Work Group members openly laughed at the suggestion. There was universal agreement that Work Group members' organizations do not use patient identifiable information in this manner.

### **Exchange of Birth Information**

This scenario was not explicitly about the exchange of birth-related information that is initiated by the birth of a child (e.g., vital records). However, we used the scenario to discuss issues related to the exchange of information required with the birth of a child. Minnesota has 108 hospitals that provide birth services, and all 108 hospitals electronically file birth records (both civil registration and medical information). However, the information system for filing vital records is a separate system and is not connected to the electronic health records.

The current process for filing vital records data begins with hospital staff completing a paper form that gathers all necessary information for the required report. Some information for the form is acquired from the electronic health record, while other information is obtained from an interview with the mother. Once the form is completed, it is entered into a database for electronic submission to the Minnesota Department of Health.

A number of issues were identified with trying to integrate the vital records reporting system with hospitals' electronic health records. Many Work Group members questioned the value of trying to integrate the systems, and believed that their electronic health records would not have much of the required information. One of the reasons that hospitals' electronic health records do not contain the required information is that some of the information is about prenatal care and is likely found in a clinic's electronic health record. The clinic's health record may or may not be available to the hospital. This issue highlights the utility of having complete health records for patients.

A second issue raised was the cost, time and resources required to integrate the systems. While these issues represent a significant barrier to integrated, interoperable information systems, they are not privacy and security concerns. The Work Group expressed reservations about the adequacy of existing standards (e.g., HL7) for exchanging standard messages with vital records. As with other standard transactions and messages, the Work Group was skeptical about the extent of standardization of the data required for the exchange. The Work Group also worried about the cost and effort to modify their systems and reporting capabilities as either the messaging standard changed (e.g., HL7) or vital records altered its reporting requirements. Hence, the Variations Work Group was uneasy about the ability to integrate their electronic health records with vital records, but their most significant concerns were related to resources and not privacy or security.

### **Impact of Key Issues**

**Access to Electronic Health Records for Healthcare Operations:** In general, most organizations do not provide access to electronic health records for health care operations, especially the health care operations described in this scenario. The organizations have well defined processes for reviewing data requests for health care operations to ensure appropriateness and compliance with regulatory requirements (e.g., minimum necessary).

**Use of Health Information for Fundraising:** No organization provided access to electronic health records for fundraising. As with health care operations, organizations have well defined processes for reviewing data requests for fundraising to ensure appropriateness and compliance with regulatory requirements (e.g., HIPAA Privacy regulations). Unlike their use of individually identifiable health information for health care operations,

organizations do not use individually identifiable health information to specifically target sub-populations of patients (e.g., birth mothers) for fundraising activities.

**Use of Health Information for Marketing:** All Work Group members stated that their organizations do not use individually identifiable health information for marketing.

**Exchange of Birth Information:** All 108 hospitals that report vital record data, including the medical information, do so electronically. However, the reporting system lacks any integration with their electronic health records. The Variations Work Group questioned if their electronic health records would have enough of the required information to justify the time and resources required to integrate the systems. Similarly, the group questioned the adequacy of the standards for integrating the systems.

**Variations in Business Practice**

There are not significant variations in the business policies and practices for using individually identifiable health information for health care operations, fundraising, or marketing. There are variations in how organizations document and track their patients' interests in receiving such communications. Some organizations provide patients the opportunity to opt out of the communications as part of their consent process, while other organizations track patients' requests to opt out of future communications as the requests are received. Similarly, some organizations document patients' desires to opt out of communications centrally in the electronic health record, while others document patients' desires locally at the source of the communication.

---

**APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario.

**Information Audits that Record and Monitor Activity**

Auditing the use of demographic information and health information as described in this scenario is generally limited to complaint-based auditing. Work Group members discussed their organizations' need to focus their auditing on uses and disclosures of data with the greatest risk of inappropriate activity. In the Work Group's experience, the activities of this scenario are not the greatest risks; their organizations have not received many complaints related to activities described in this scenario, nor have they found many problems with inappropriate activities. The detailed scrutiny that data requests receive prior to making the data available is seen as a sufficient control on inappropriate uses of the data. Additionally, the organizations investigate any complaints received and take action as appropriate. The combination of carefully reviewing the proposed uses of data and using complaint-based auditing has been a cost-effective method of ensuring that the data are used appropriately.

---

**IDENTIFIED BARRIERS OR BEST PRACTICES**

---

Other than the disclosure of demographic information for marketing (i.e., Purpose #4 in the scenario), there is no data exchanged within this scenario. Given that Work Group members do not engage in the marketing activities of this scenario, the Work Group did not identify barriers or best practices for the exchange of health information.

However, the Work Group discussion pointed out the value of having a formal process for requesting identifiable health information and demographic information, which requires the requester to specify in detail

what data are needed and how the data will be used. This valuable process ensures that health information is used appropriately and serves as a cost-effective control on inappropriate uses of health data.



## ANALYSIS OF SCENARIO #13 BIOTERRORISM EVENT

---

### SCENARIO OVERVIEW

---

*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.*

To provide structure for the discussion and analysis of this scenario, staff identified one key issue and seven questions for consideration (see Expanded Scenario #13). The key issue identified was the aspect of the scenario that was anticipated to be most significant to the scenario and likely to trigger specific business policies and practices. The identified issue was:

- **Exchange of Health Information in a Potential Bioterrorism Event:** This issue was a key issue because a potential bioterrorism event represents a significant threat to the public's health. Law enforcement and public health need the ability to quickly exchange health information to appropriately address the threats of bioterrorism events. We anticipated that the Minnesota Department of Health has specific statutory authorities for the use and disclosure of individual-identifiable health information during a potential bioterrorism event.

The seven questions for consideration were intended to focus the discussion and attempted to:

- Determine who would report the initial cases of anthrax, who would receive the report of anthrax, and how the information would be reported.
- Assess how and why individual-identifiable health information would be exchanged.
- Identify the most significant privacy/security concerns with the exchange of individual-identifiable health information during a potential bioterrorism event.
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

### GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

We analyzed this scenario with the Minnesota Department of Health's Office of Emergency Preparedness, which coordinates the Department of Health's preparedness activities and assists local public health agencies,

hospitals, health care organizations, and public safety officials in their efforts to plan for, respond to, and recover from public health emergencies.

Recognizing that the scenario was prepared as part of a national project, there were a number of issues that needed to be modified/clarified to make the scenario more consistent with Minnesota. Some important modifications/clarifications are:

- **Type of Anthrax:** The scenario does not identify if the anthrax is cutaneous anthrax or inhalational anthrax. However, the low incidence of anthrax means that even a single case of anthrax would be suspicious. Naturally acquired **cutaneous anthrax** is extremely rare. Unless the affected individual worked with animals, animal hides, or wool, cutaneous anthrax would raise suspicions of criminal behavior. **Inhalational anthrax** would immediately raise suspicions of criminal behavior. We generally assumed that the cases of anthrax within the scenario were inhalational anthrax, although the difference in MDH's response would be minimal unless the affected individual worked with animals or animal hides.
- **Reporting Anthrax:** Minnesota Rules, Chapter 4605, require physicians, health care facilities, medical laboratories, veterinarians and veterinary medical laboratories to report anthrax to the Minnesota Department of Health (MDH) immediately and by telephone. MDH has Infectious Disease Epidemiology, Prevention and Control staff available for disease consultation and reporting 24 hours a day, 7 days a week. Consequently, the first report of anthrax would be to the MDH rather than to a local public health department. In fact, local public health departments would only be made aware of the anthrax cases through communications from MDH.
- **Declaring a State Emergency:** A state emergency would only be declared in order to: 1) invoke emergency management powers under Minnesota Statutes, Chapter 12, Minnesota Emergency Management Act of 1996 (e.g., make, amend, or rescind administrative rules); and/or 2) to request assets from the federal government because Minnesota has exhausted its resources. Assuming that the scenario has two cases of anthrax (one in each county), the situation would probably not require the declaration of an emergency. However, if the situation changed and it was necessary to declare an emergency, Minnesota law addresses this situation. The Governor is provided broad authority and emergency management powers to address public health emergencies under Minnesota Statutes, Chapter 12. The law has no privacy or security barriers that would restrict or prevent the necessary exchange of health information.

Beyond these clarifications, the discussion of the scenario revealed that MDH's actions and information exchange would depend significantly on the specific facts uncovered during the investigation of the anthrax cases. Consequently, the discussion applied the general authorities and activities of MDH to the scenario.

**Disclosure of Health Data in General**

The health information collected by MDH on anthrax cases is classified as "Health Data" as defined under Minnesota Statutes § 13.3805, Subd. 1, (2):

*"Health data" means data on individuals created, collected, received, or maintained by the Department of Health, political subdivisions, or statewide systems relating to the identification, description, prevention, and control of disease or as part of an epidemiologic investigation the commissioner designates as necessary to analyze, describe, or protect the public health.*

Minnesota Statutes § 13.3805, Subd. 2 defines health data as private data and generally restricts its disclosure without specific authority. However, the Statute provides the Commissioner of Health broad authority to disclose the information in order to appropriately address public health threats. Specifically, the information may be disclosed to:

- The patient's physician as necessary to locate or identify a case, carrier, or suspect case, to establish a diagnosis, to provide treatment, to identify persons at risk of illness, or to conduct an epidemiologic investigation;
- Assist the Commissioner to locate or identify a case, carrier, or suspect case;
- Assist the Commissioner to alert persons who may be threatened by illness as evidenced by epidemiologic data;
- Assist the Commissioner to control or prevent the spread of serious disease; or
- Assist the Commissioner to diminish an imminent threat to the public health.

In general, these authorities would be sufficient to permit MDH to disclose health data as needed to address this scenario. Additionally, MDH could also disclose the health data with the affected individual's consent and would seek such consent if it would facilitate the timely release of information.

**Disclosure of Health Data to Health Care Providers and Local Public Health**

Immediately upon a report of inhalational anthrax, MDH would begin communicating with the health care provider and facility making the report. The communications would address issues such as:

- Collaborating with the patient's physician to identify appropriate courses of treatment;
- Working with the staff and laboratory to ensure that an appropriate lab sample is secured for additional analysis;
- Providing information to the hospital's infection control practitioners on any necessary actions; and
- Gathering a patient history that is as complete as possible.

One of MDH's main concerns would be identifying the source of the anthrax and others who may have been infected from the same source. A complete patient history would be critical in identifying the source, particularly if the two cases have a common origin. One of the difficulties in collecting a complete patient history is that the patient is likely to be very sick, on a ventilator, and may not be able to provide the information. Because the patients may be too ill to provide a complete history, MDH would want to talk with any hospital staff or medical personnel who have interacted with the patient. These conversations would likely reveal the patients' identities and condition.

MDH's Office of Emergency Preparedness operates the Health Alert Network, which provides primary information and timely communications about public health threats. This e-mail tool allows MDH to communicate immediately with local public health agencies, clinicians, hospitals and other partners in Minnesota's health care system. Information about the anthrax cases would be distributed via the Health Alert Network to help providers understand the threat and to be alerted to additional possible cases. It is unlikely that this communication would directly identify the anthrax patients by name, however the description of the cases would have many identifying elements (e.g., age, gender, information about where the exposure may have occurred, etc.).

Additionally, MDH would contact local health departments to assist in identifying additional cases of anthrax. Whether or not the local health departments would need to have information directly identifying the anthrax patients would depend on what was known about the source of exposure. If identifying the patients is necessary to find additional cases of anthrax, then their identities would probably be disclosed. Otherwise, the communications would just provide details of the case without directly naming the two patients.

It is anticipated that most of the communications and exchange of patients' health data with providers and public health would be done via telephone and fax. These methods of communication and exchange are not preferred because of privacy and security concerns, but rather because the urgency of the situation requires immediate, interactive communications that facilitate the quick and accurate exchange of information.

#### **Disclosure of Health Data to Law Enforcement**

Inhalational anthrax, or cutaneous anthrax in individuals not associated with animals or animal hides, would almost certainly indicate criminal behavior. Therefore, MDH would communicate with law enforcement alerting them to the potential crime. Ideally, MDH would ask the patients' physicians to communicate to the patients that their information is going to be provided to law enforcement as part of a criminal investigation. The hospital would then report the potential crime to local law enforcement, while MDH would report the potential crime to state and federal law enforcement. MDH would provide law enforcement with any information that would assist in the investigation of the crime, including patient identifying health data.

#### **Disclosure of Health Data to Others**

As stated previously, MDH would want to construct a complete history of the patients' activities to identify the source of their infections and any other infected individuals. Because the two patients may not be able to provide that history, MDH would want to contact family members and others who may be helpful in identifying the source of the exposure. Additionally, MDH may want to determine if family members, friends, or others have symptoms that would be consistent with inhalational anthrax. In the course of its investigation and discussion with those individuals, MDH would probably need to disclose some of the infected patients' identities and the fact that they have anthrax.

In general, MDH would make every effort to protect the anthrax patients' identities. However, protecting the public's health takes precedence over the individuals' privacy. The Commissioner of Health has broad authority to use and disclose patient-identified health data. If circumstances arise within a potential bioterrorism event that requires the Commissioner to disclose information about the patients' identities to protect the public, then their identities will be disclosed as needed.

#### **General Privacy Concerns**

The Office of Emergency Preparedness identified two general privacy concerns in addressing this scenario. The first concern relates to the Commissioner of Health's authority. The Minnesota Legislature has provided the Commissioner of Health extremely broad statutory authority to address public health threats. The Department of Health has always strived to exercise that authority judiciously and execute its responsibilities within the public's trust and the Legislature's expectations. Whether planning for a bioterrorism event or responding to an actual public health outbreak, MDH wants to exercise its responsibilities and authorities in a thoughtful, methodical, and prudent manner, including its discretion to disclose patient-identified health data.

The second general privacy concern relates to the practical ability to protect the anthrax patients' identities. Although MDH would only disclose the patients' identities as necessary to protect the public's health, it is doubtful that the patients' identities would or could remain confidential. Within this scenario, a large number of people would know the patients' identities – family, friends, hospital and medical staff, public health and various levels of law enforcement. Any of these individuals may have legitimate reasons for identifying the patients' identities, including the patients' families. If a bioterrorism event involving inhalational anthrax occurs, the news media will attempt to contact anyone and everyone associated with the event. It is unlikely that patients' identities will not be ascertained and reported. In fact, the patients' families may believe that it is important for others to know the details of the event. Consequently, the patients' identities within this scenario will likely not remain confidential.

**Impact of Key Issues**

**Exchange of Health Information in a Potential Bioterrorism Event:** Minnesota law provides the Commissioner of Health broad authority to use and disclose patient-identified health data to protect the public's health. MDH's Office of Emergency Preparedness reported no privacy or security barriers to the exchange of patient-identified health data if faced with a potential bioterrorism event such as inhalational anthrax. While every effort would be made to protect patients' identities in responding to the situation of this scenario, MDH may need to disclose patients' identities as part of its investigation to identify the source of the infections and to identify additional cases.

---

**APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

The Office of Emergency Preparedness was asked to consider the intersection between the project's nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario. No additional issues were identified.

---

**IDENTIFIED BARRIERS OR BEST PRACTICES**

---

No privacy or security barriers to the appropriate exchange of patient-identified health information were identified in the analysis of this scenario. The Commissioner of Health has broad authority to respond to public health outbreaks and threats. This authority includes the ability to disclose patient-identified health data for the purposes anticipated by this scenario. Thus, while every effort would be made to protect the privacy of anthrax patients' identities, the information may be disclosed if necessitated by situational analysis during the event. Additionally, the Governor has broad emergency management powers for declaring and addressing public health emergencies. Nothing in the authority granted to the Governor or the Commissioner of Health represents a privacy or security barrier to appropriately exchanging health information in response to a bioterrorism event.

## ANALYSIS OF SCENARIO #14 EMPLOYMENT INFORMATION

---

### SCENARIO OVERVIEW

---

*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 ED has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information electronically to the HR department.*

To provide structure for the Variation Work Group members' discussion and analysis of this scenario, staff identified four key issues and four questions for consideration (see Expanded Scenario #14). The key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario, likely to trigger specific business policies and practices, and relevant for identifying variations in processes between work group members. The identified issues were:

- **Exchanging Health Information with a Patient's Employer:** This issue was identified as a key issue because patients often have concerns about disclosing identifiable health information for activities other than treatment. Patients are particularly concerned about the disclosure of their health information to their employer. We also anticipated that organizations have specific policies concerning the disclosure of information for activities that are not treatment, payment, or operations.
- **Secure Exchange of Information:** This issue was identified as a key issue because patients and organizations are growing increasingly concerned about the security and confidentiality of data, particularly when exchanged electronically. We anticipated that organizations have specific policies to address security concerns when electronically exchanging data.

The four questions for consideration were intended to focus the Work Group's discussions and to:

- Determine how organizations provide employers a return-to-work letter, including:
  - Who is provided the letter
  - How the letter is transmitted
  - Any authorization requirements
  - Assess organizations' willingness to provide the information via e-mail
- Identify limitations in providers' ability to discuss follow-up issues with an employer based on the letter
- Describe the intersection of the scenario with the nine privacy and security domains used within the project

## GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

In general, Variation Work Group members agreed that it was common for patients to request letters that:

- indicate the patient's fitness to return to work; and/or
- identifies any health-related limitations for work activity (e.g., may not lift more than 10 pounds)

Variations Work Group members' organizations have very similar policies and processes for addressing the situation described in this scenario.

### Creation and Content of Letter to an Employer

The Variations Work Group identified three methods that their organizations use to create letters or communications to a patient's employer. Some organizations described having a standard form letter in their electronic health record that can be easily completed by a provider. The provider includes the appropriate information in the form and prints the letter. The electronic health record also maintains a record of the letter created. A second, similar method described by some organizations involved manually completing a standard paper form. The provider completes the paper form, and then, a photocopy of the letter is placed in the patient's medical record. Some organizations described a third method occasionally used by emergency department providers. Given the time constraints of the emergency department, some providers will simply write the information to be communicated on a prescription pad and then document the information in the patient's record.

Regardless of the method used to generate the letter, all Work Group members stated that the letter would contain as little health information as possible. For example, a letter stating that a person was fit to return to work may contain no health information beyond the date the patient was seen and the fact that the patient was determined fit to work. Similarly, a letter describing health-related limitations would focus on the nature of the restrictions and not on the underlying medical condition. All Work Group members agreed that a letter would contain the minimum necessary health information.

### Transmission of Letter to an Employer

All Work Group members stated that the usual method for transmitting the letter to the employer was via the patient. After the letter is created, it is signed by the provider and given directly to the patient. The patient may then provide the letter to the employer as appropriate.

There are two reasons that were given for providing the letter directly to the patient. First, it is one of the easiest and fastest methods for ensuring that the information is delivered to the correct location and is handled appropriately. By giving the information to the patient, providers can be confident that the information will be handled in a manner consistent with the patient's wishes. The second reason for providing the letter directly to the patient is to avoid addressing patient consent requirements associated with communicating directly with an employer. All Work Group members organizations require patient authorization/consent (under the HIPAA Privacy regulations and Minnesota Statutes § 144.335) to provide the information directly to the employer. Hence, it is easier to provide the information directly to the patient and to let the patient take responsibility for it.

Work Group members were asked about their process when an employer wants the information sent directly to them. The organizations stated that they must secure the patient's consent to provide the information. Then, they mail the letter to the employer using the US Postal Service. If the patient insisted that it be sent directly to the employer and if needed urgently, the providers may fax the information to the employer.

All provider organizations on the Work Group stated that their organizations would prohibit, or at least not support, the information being sent to the employer via e-mail. All Work Group members said their

organizations prohibit sending health information in unsecured e-mail. Given the administrative difficulty of implementing secure e-mail, some organizations have a blanket policy against including identifiable health information in e-mails. Other organizations have mechanisms to permit secure e-mail, but discourage its use for routine activities. These organizations believe that the procedures for ensuring secure e-mail are cumbersome and the risk of e-mail being improperly secured is too high. Hence, a computer-literate physician may send a letter to an employer via secure e-mail; however, this communication would be an exception and not the rule.

**Follow-Up Discussions with an Employer**

After receiving the letter from the provider, it is common for employers to telephone providers to get additional information. Often the employer wants additional information about the underlying health condition that is related to the letter. Given that providers have policies to limit any health information included in the letter to the absolute minimum necessary, the employer’s interest in trying to receive additional information may not be surprising.

All Variations Work Group members stated unambiguously that while their organizations would confirm the contents of the letter, and they would not discuss any health information about the patient without the patient’s consent.

**Impact of Key Issues**

**Exchanging Health Information with a Patient’s Employer:** In general, providers do not exchange the information described in this scenario directly with employers. The minimum necessary health information is placed in a letter and then provided directly to the patient who takes responsibility for the letter. If information is to be provided directly to an employer, the provider must first obtain the patient’s written consent authorizing the disclosure of information to the employer.

**Secure Exchange of Information:** Organizations are concerned about the security of the exchange of health information. These security concerns cause providers to give the letter to the patient and to let the patient be responsible for their own information. In direct communications, providers use the US mail and fax to send information to employers. Providers have generally found secure e-mail to be difficult to implement and usually prohibit, or strongly discourage, the transmission of health information through e-mail.

**Variations in Business Practice**

The Work Group did not identify variations for the most significant issues of this scenario. All organizations agreed:

- Any health information included in the letter would be the minimum necessary;
- The letter would generally be provided directly to the patient and not the employer;
- If the letter were sent directly to the employer, organizations would obtain the patient’s consent to disclose the information; and
- Providers would not have follow-up discussions with an employer without the patient’s consent.

The Work Group discussion did identify minor variations in the process organizations use to address this scenario, specifically regarding the organization’s technological capabilities. The variations include:

- Three methods for creating the letter, including 1) directly from the electronic health record with a standard letter; 2) manually completing a paper form; and 3) manually putting the information on a prescription pad in the emergency department.

- Use of secure e-mail. Some organizations prohibit sending this information via e-mail, whether or not they have a mechanism for secure e-mail. Other organizations strongly discourage sending this information via secure e-mail, but admit that a provider could send it via secure e-mail.

---

## APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario.

### **State Law Restrictions**

Work Group members pointed out that some aspects of this scenario would be evaluated differently if it were a Workers Compensation claim. First, the HIPAA Privacy regulations would no longer be applicable. Second, Minnesota Statutes § 176.138(a) states:

*Notwithstanding any other state laws related to the privacy of medical data or any private agreements to the contrary, the release in writing, by telephone discussion, or otherwise of medical data related to a current claim for compensation under this chapter to the employee, employer, or insurer who are parties to the claim, or to the Department of Labor and Industry, shall not require prior approval of any party to the claim....*

Hence, Work Group members' organizations do not obtain patient consent to release information related to a Workers Compensation claim as long as the information to be released is related to the claim.

---

## IDENTIFIED BARRIERS OR BEST PRACTICES

---

The greatest barrier to electronically exchanging the return-to-work letter with an employer is organizations' policies prohibiting the inclusion of patient identifiable information in unsecured e-mail. Many of the Work Group members' organizations do not support the use of secure e-mail. They have found it difficult to implement and use. Given the organizations' ongoing concerns with e-mail security they find other ways to deliver the letter to the employer.

Even if the return-to-work letter could be easily sent via e-mail, the organizations would need to alter their business practices. They would need to obtain the patient's consent to release the information. The current method of providing the letter to the patient avoids having to address this issue. Thus while patient consent does not create a barrier, it does create another requirement that would need to be satisfied to send the letter electronically.

## ANALYSIS OF SCENARIO #15 PUBLIC HEALTH - SCENARIO A ACTIVE CARRIER, COMMUNICABLE DISEASE NOTIFICATION

---

### SCENARIO OVERVIEW

---

*An Active TB Patient has decided to move to a desert community that focuses on spiritual healing. The TB is classified MDR (multi-drug resistant). Patient purchases a bus ticket - the bus ride will take a total of nine hours with two rest stops. State A is made aware of Patient's intent two hours after the bus with Patient leaves. State now needs to contact the bus company and State B with the relevant information. State A may need to contact every state along the route.*

To provide structure for the discussion and analysis of this scenario, staff identified one key issue and six questions for consideration (see Expanded Scenario #15). The key issue identified was the aspect of the scenario that was anticipated to be most significant to the scenario and likely to trigger specific business policies and practices. The identified issue was:

- **Sharing Individual-Identifiable Communicable Disease Information across State Borders:** This was a key issue because State Health Departments often need to share individual-identifiable health information to protect the public's health and prevent the spread of disease. Consequently, we anticipated that the Minnesota Department of Health has specific policies and procedures for exchanging individual-identifiable health information with other states.

The six questions for consideration were intended to focus the discussion and attempted to:

- Determine what individual-identifiable health information would be shared and with whom the information would be shared.
- Explore the mechanisms for sharing appropriate individual-identifiable health information.
- Assess any limitation or barriers to sharing the appropriate information.
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

### GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

We analyzed this scenario with the Tuberculosis Unit of the Infectious Disease Epidemiology, Prevention and Control Division within the Minnesota Department of Health (MDH). In Minnesota, all cases of tuberculosis (TB) must be reported to MDH under Minnesota Statutes § 144.4804.

One of MDH's main responsibilities is to protect the public's health and to prevent the spread of disease. Therefore, their initial analysis of this scenario focused on determining the actions necessary to prevent the spread of disease. Even before considering what information might need to be exchanged, MDH identified a number of important aspects of the scenario that would influence their actions and would need to be clarified:



- MDH would want to determine if the patient was infectious. The fact that the patient has active TB does not imply that they are infectious. For example, the person would only be infectious if the TB was in the patient's lungs.
- Given that MDH already knows that this case is multi-drug resistant (MDR) TB, they assume that they would have a lot of other medical information regarding the patient. Laboratories generally require a minimum of 3-4 weeks to confirm MDR TB. Hence, MDH would have already received the initial report of the case and have been following the case for at least a month.
- The fact that this was a nine-hour bus ride was an important detail. TB is not easily transmitted and generally requires prolonged exposure for the disease to be transmitted. Consequently, the time spent at rest stops would not represent a significant exposure risk. Similarly, passengers on the bus for less than eight hours would generally be at a lower risk of infection and would not normally need evaluation.

Although the exact actions of MDH would depend on the unspecified details of the case, the general policies and practices are described below.

### **Disclosure of Health Data in General**

The health information collected by MDH on TB patients is classified as "Health Data" as defined under Minnesota Statutes § 13.3805, Subd. 1, (2):

*"Health data" means data on individuals created, collected, received, or maintained by the Department of Health, political subdivisions, or statewide systems relating to the identification, description, prevention, and control of disease or as part of an epidemiologic investigation the commissioner designates as necessary to analyze, describe, or protect the public health.*

Minnesota Statutes § 13.3805, Subd. 2 defines health data as private data and generally restricts its disclosure without specific authority. However, the Statute permits the Commissioner of Health to disclose the information to: 1) the patient's physician; and 2) to prevent the spread of disease. These permissions are in Minnesota Statutes § 13.3805, Subd. 2, (2) and (3):

*(2) The commissioner or a local board of health as defined in section 145A.02, subdivision 2, may disclose health data to the data subject's physician as necessary to locate or identify a case, carrier, or suspect case, to establish a diagnosis, to provide treatment, to identify persons at risk of illness, or to conduct an epidemiologic investigation.*

*(3) With the approval of the commissioner, health data may be disclosed to the extent necessary to assist the commissioner to locate or identify a case, carrier, or suspect case, to alert persons who may be threatened by illness as evidenced by epidemiologic data, to control or prevent the spread of serious disease, or to diminish an imminent threat to the public health.*

### **Exchanging Health Data with the Patient's Physician**

Given that this case has been reported and determined to be multi-drug resistant, MDH would have already started regular interaction with the patient's physician and collected a substantial amount of the TB patient's health data. The purpose for the on-going exchange of information with the patient's physician is to track the patient's status, follow treatment progress, and ensure conformance with established treatment/drug guidelines. Only information related to the patient's TB is exchanged (e.g., treatment dates, monthly lab results, and medication regimens).

The information is exchanged via telephone, fax, and US mail. The exact method for exchanging data depends on the patient's status and stage of the treatment, which may last from six to twenty four months.

When a case is initially reported, communications between the patient's physician and MDH will generally occur via telephone and fax. As treatment progresses, there may be less urgency to the communications and the exchanges will often happen by US mail.

Very little information is exchanged via e-mail. MDH does not consider e-mail to be a secure mode of communication and prohibits exchanging patient-identified data via e-mail. The Tuberculosis Unit is also cautious in exchanging information related to a patient's case even if the information does not specifically identify the patient. For information to be sent via e-mail, the Tuberculosis Unit uses the following rule: "If a trained epidemiologist could use the data to determine who is being referenced, then the information can not be sent via e-mail."

### **Disclosing Health Data State B**

MDH would disclose individual-identifiable health data to the appropriate health authority in State B (e.g., State Department of Health). The purpose of this disclosure would be to prevent the spread of disease and to diminish an imminent threat to the public's health. Also, State B would be provided the information to allow them to properly follow-up on a case of TB in their state.

The Tuberculosis Unit maintains a list of contacts for every state. Once they were aware that the patient was moving to State B, they would telephone the appropriate person within State B in order to:

- inform State B that a TB case is moving to their state;
- verify the fax number for sending information to State B; and
- ensure that State B has received the faxed Interjurisdictional Tuberculosis Notification form and any other faxed information (see attached form).

Before sending the information to State B, MDH would contact the patient's physician and local health department to ensure that the most recent information (e.g., lab results and medication regimen) was being disclosed.

### **Disclosing Health Data to Other States**

MDH would not disclose any individual-identifiable health data to the other states along the bus route. There would be no need for these other states to receive any information about the patient. Even if the patient were highly infectious and there was concern that someone in one of the other states could be infected, there would be no reason that the State would need the original patient's identifying information.

Minnesota, as the state of origin, would be responsible for conducting a contact investigation, if there was concern that others on the bus may have been infected. In these circumstances, MDH would work with the other States to identify individuals that have been exposed and need to be tested. MDH would provide the other states information about the case, such as the type of drug resistance and dates of exposure. However, the information would not need to identify the case-patient.

### **Disclosing Health Data to the Bus Company**

The bus company would only be contacted as necessary to prevent the spread of TB. That is, MDH may need to work with the bus company as part of a contact investigation to determine if other individuals have been exposed and possibly infected. The investigation would occur only if the patient was infectious and MDH believed that there was a risk that others may be infected. Under these circumstances, MDH would want to verify that the patient was on the bus, obtain a manifest of passengers, and determine who sat closest to the patient. In the course of working with the bus company, the patient would be identified and the fact that it was a TB investigation would be revealed. No other information about the patient would be disclosed to the bus company.

**Accessing Health Data through Electronic Health Records**

The most common exchange of health data related to this scenario is between MDH and the patient’s physician. Hence, we asked the Tuberculosis Unit if it would be helpful to be able to access the health data directly via an electronic health record and if there would be any concerns about electronically accessing that data.

The Tuberculosis Unit questioned if all of the information normally reported to MDH would be included and accessible through an electronic health record. Additionally, the Tuberculosis Unit stressed that it is not simply engaged in passive data collection from physicians. The exchanges with physicians are active conversations related to practice guidelines, drug combinations, and patient treatment. Consequently, the accessibility of electronic health records may facilitate the exchange of information, but it is unlikely to replace interactive conversations with physicians.

The Tuberculosis Unit was also concerned about getting access to too much data. MDH only collects health data related to the patient’s TB and does not collect or want information related to other aspects of the patient’s medical care. Therefore, it was concerned that any access through electronic health records would need to ensure that the accessible data were limited to appropriate TB-related data.

**Impact of Key Issue**

**Sharing Individual-Identifiable Communicable Disease Information across State Borders:** The Commissioner of Health has broad authority to disclose health data to control and prevent the spread of serious disease. Within this scenario, that authority permits MDH to disclose individual-identifiable health data to other State Health Departments to ensure that TB cases are properly transferred between States. MDH has a standard process for disclosing this information, including a list of state contacts, standard forms, and procedures for sending data (e.g., telephone and fax contacts). There are no significant privacy/security barriers to appropriately exchanging these data.

---

**APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

The Tuberculosis Unit was asked to consider the intersection between the project’s nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario. No additional issues were raised.

---

**IDENTIFIED BARRIERS OR BEST PRACTICES**

---

No significant privacy or security barriers were identified in appropriately exchanging data within this scenario. The only privacy/security issue related to the exchange of this information is the security of e-mail. Currently, all individual-identifiable health data is exchanged via telephone, fax, and US mail, because MDH does not consider e-mail to be a secure method for exchanging individual-identifiable health data. Consequently, this removes a common and potentially useful method of communicating and exchanging information.

## ANALYSIS OF SCENARIO #16 PUBLIC HEALTH - SCENARIO B NEWBORN SCREENING

---

### SCENARIO OVERVIEW

---

*A newborn's screening test comes up positive for a rare genetic disorder and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder. 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 rare genetic disorder and notifies the physician that the child is eligible for those programs. One of the services that the mother uses from the state is regularly purchasing special food products for persons with PKU.*

To provide structure for the discussion and analysis of this scenario, staff identified three key issues and six questions for consideration (see Expanded Scenario #16). The key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario and likely to trigger specific business policies and practices. The identified issues were:

- **Communicating Newborn Screening Results to Treatment Providers:** This issue was identified as a key issue because timely communication about metabolic disorders identified through newborn screening is critical to the physical and mental welfare of infants. It was anticipated that the Minnesota Department of Health's Newborn Screening Program has well established policies and procedures for ensuring timely and accurate communications with health care providers responsible for addressing infants' metabolic disorders.
- **Communicating Newborn Screening Results to Governmental Programs and Social Support Service:** This issue was identified as a key issue because the metabolic disorders identified through newborn screenings are rare disorders that are outside most primary care providers' usual experience. Therefore, it was anticipated that newborn screening program may exchange information or otherwise help facilitate connecting families with programs and services that provide assistance to children with metabolic disorders.
- **Secure Exchange of Patient-Identified Data:** This issue was a key issue because patients and organizations are growing increasingly concerned about the security and confidentiality of data, particularly when exchanged electronically. We anticipated that Minnesota Department of Health's Newborn Screening Program has specific policies and practices to address security concerns when electronically exchanging data.

The six questions for consideration were intended to focus the discussion and attempted to:

- Determine who would receive newborn screening results, how the results would be exchanged, and any security measures implemented to protect the privacy and confidentiality of the newborn.
- Identify the most significant privacy/security concerns with collecting and exchanging individual-identifiable health information related to the newborn screening program.

- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

## GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

We analyzed this scenario with the Minnesota Department of Health's Newborn Screening Program, which is responsible for operating Minnesota's newborn screening activities. The responsibilities and authorities given to the Minnesota Department of Health (MDH) are found in Minnesota Statutes § 144.125 – 144.128 and Minnesota Rules, Chapter 4615. This scenario focused on phenylketonuria or PKU; however the policies and practices described are applicable to almost all of the 53 heritable and congenital disorders included in Minnesota's newborn screening program.

### **Newborn Screening Background**

Minnesota has approximately 72,000 births per year which occur at approximately 109 birthing centers. Minnesota law mandates that all newborns be screened for metabolic disorders unless a parent objects in writing. Approximately 700 infants per year are presumptively positive with 100 infants per year being confirmed positive for a heritable or congenital disorder, meaning that nearly all of the program's test results are normal. In the case of a normal screening result, the lab results are generated into a report that is mailed, via the US mail, to the hospital or other provider that submitted the newborn's blood spot specimen. The hospital is then responsible for forwarding the lab results to the appropriate primary care physician responsible for the infant's on-going medical care.

Given the large number of births, screenings, and letters communicating results, it is important that the work flow and business processes are organized to ensure that all normal results can be reported quickly and efficiently. Thus, the screening program's use of US mail to report normal lab results is not a privacy and security measure, but rather a business decision to have uniform process for communicating results.

### **Exchange of Presumptive Positive Screening Results with Providers**

When MDH identifies a positive test result, staff immediately begins the process of notifying appropriate health care providers. In fact, the notification process frequently starts before all tests are completed. The health care providers contacted, methods of communication, and order in which providers are notified are described in the following steps:

- **Step 1:** MDH telephones the infant's primary care provider as identified by documentation that accompanied the blood spot specimens. If the primary care provider is unavailable, MDH identifies a primary care provider within the same clinic. Additionally, MDH faxes the primary care provider the following materials:
  - A preliminary copy of the infant's lab results, identifying the positive test;
  - Parent and provider fact sheets that provide additional information about the relevant disorder, identify next steps for parents and providers, and assist in locating additional information;
  - Contact information for specialists experienced in treating the identified disorder; and
  - A form that establishes that the primary care provider has a treatment relationship with the infant and will be responsible for contacting the family and starting the infant's treatment. This form must be completed and faxed back to MDH to document the treatment relationship between physician and the infant.

- **Step 2:** In Minnesota, the specialists that treat metabolic conditions provide an on-call physician for each day of the week to help assist primary care providers who are notified of a presumptive positive test result. This on-call specialist is telephoned and informed of the positive result, faxed a copy of the preliminary lab result, and given contact information for the infant’s primary care provider.
- **Step 3:** MDH and approximately 45 health professionals related to the treatment of metabolic disorders have established a secure web-based communication system for the active and rapid electronic exchange of information. This tool allows MDH and the specialists to enter initial test results, confirmatory test results, initial status of the infant (if known), and the primary care physician’s contact information. Once MDH reports the initial, preliminary positive result to this communication system, it automatically generates an e-mail to the specialists alerting them to a new case. The specialists can use a secure connection to login to the system and access the available information.

The goal of these communications with primary care providers and specialists is to ensure that the infant begins receiving treatment as quickly as possible. If the affected infants are left untreated, these disorders can lead to illness, physical disability, mental retardation, or death. However, medication and changes in diet can help prevent most health problem caused by the disorder, so it is critical that treatment begin quickly.

Maintaining the privacy and security of information exchanged within this scenario is an important consideration for MDH and the specialists that treat metabolic disorders. Their attention to privacy and security issues can be seen through their implementation of a secure metabolic care communication system. Yet, much of the information related to this scenario is communicated by telephone and fax. These methods of communication are used because telephone and fax allow for rapid, convenient, and secure communication of urgent information. In the case of PKU, the average time from birth to treatment is four days. Hence, privacy and security issues are not dictating the methods of communication, but rather the proven utility of the telephone and fax communications are determining how information is exchanged.

**Disclosure of Health Data to Law Enforcement**

Occasionally, the primary care provider identified in the documentation provided with the blood spot specimens is not the infant’s physician and MDH cannot establish a treatment relationship between a provider and the affected infant. MDH regards these situations as medical emergencies and solicits law enforcement’s assistance in locating the mother and alerting the family of the need to begin treatment. In order for law enforcement to render effective assistance, MDH needs to provide them certain patient-identified data, such as mother and child’s name, a general description of the medical emergency and the importance of seeking immediate treatment.

**Disclosure of Health Data to Others**

MDH’s Newborn Screening Program is intended to provide primary care and specialty physicians an early alert of infants with metabolic conditions. The alert ensures that a treatment relationship is established between a primary care physician and infants with metabolic disorders. It also ensures that the primary care physicians have the knowledge necessary to follow through with the next treatment steps including confirmatory testing and connection to specialty care. Given the purposes and intention of the newborn screening program, the program does not generally share patient-identified data with others not involved in the infant’s treatment.

**Connection to Social Services and Other Programs**

MDH’s Newborn Screening Program helps connect the families of infants with metabolic disorders with social and support services by sponsoring a metabolic care coordinator position in one of Minnesota’s two metabolic specialty centers. This position serves as a resource for families and assists parents in identifying and enrolling in programs and relevant services. The coordinator position is located within the treatment facility

and participates in the treatment relationship similarly to a care coordinator or social worker in other care settings. MDH does not exchange patient-identified data with the care coordinator, although MDH receives aggregate data reports about the number of cases seen, number of referrals, and number of enrollments in various programs.

**Impact of Key Issues**

**Communicating Newborn Screening Results to Treatment Providers:** When MDH’s Newborn Screening Program identifies a positive test result, staff immediately begins the process of notifying appropriate health care providers. The notification process consists of notifying the primary care physician by telephone and fax, verifying a treatment relationship between the primary care provider and the infant, informing an on-call specialty physician by telephone and fax of the test result, and reporting the test results to a secure metabolic care coordination system that is linked to all of the specialists in the state. The purpose of these communications is to ensure that the infant begins receiving appropriate treatment as quickly as possible

**Communicating Newborn Screening Results to Governmental Programs and Social Support Service:** MDH’s Newborn Screening Program does not communicate test results or patient-identified data to governmental programs or support services. However, it sponsors a metabolic care coordinator position in one of Minnesota’s two metabolic specialty centers to aid families in connecting with appropriate programs and support services.

**Secure Exchange of Patient-Identified Data:** MDH’s Newborn Screening Program exchanges test results through a variety of means. Normal test results are returned via US mail to the entity submitting the blood spot specimens. Abnormal test results are immediately shared with primary care and specialty physicians via telephone and fax to ensure convenient, rapid and secure exchange. Additionally, lab results are made available to the approximately 45 health professionals dealing with metabolic disorders through a secure metabolic care coordination system that helps ensure infants begin the treatment process.

---

**APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

The Newborn Screening Program was asked to consider the intersection between the project’s nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario.

**User and Entity Authentication**

MDH’s Newborn Screening Program indicated that its main privacy/security issues are not related to the exchange of patient-identified data associated with abnormal test results, but rather to the exchange of normal test results. There are over 70,000 normal newborn screening per year. The results are mailed back to the submitting entity, usually a hospital, and that entity is responsible for forwarding the normal results to the primary care physician. However for a variety of reasons, sometimes the results are not forwarded to the primary care provider. MDH receives 200 calls per month from primary care providers requesting the newborn screening results. These requests require the Newborn Screening Program to have some method for authenticating the individuals requesting results.

The Newborn Screening Program maintains a registry of clinic fax numbers. If an individual calls and requests an infant’s test results, the caller is asked if they have a treatment relationship with the infant and to provide their clinic’s fax number. If the fax number provided is in the clinic registry, the clinic is faxed the test results. If the fax number is not included in the registry, the individual is asked to supply letterhead or other appropriate documentation indicating their clinic’s fax number. Once this information is provided, the fax number is added to the registry and the information is faxed. This authentication procedure makes two general assumptions: 1) the letterhead provided is legitimate; and 2) the provider requesting the information

truly has a treatment relationship with the infant. The process has seemingly worked well, because MDH has not had any problems with this authentication procedure even with the large number of requests from primary care providers.

---

### IDENTIFIED BARRIERS OR BEST PRACTICES

---

No privacy or security barriers to the appropriate exchange of patient-identified health information were identified in the analysis of this scenario. Information exchanged between MDH's Newborn Screening Program, primary care providers, and specialty physicians is done via telephone, fax, and secure communication systems. Much of the information about an abnormal test result is communicated through telephone and fax. The rationale for using these methods of communication is that telephone and permit rapid, convenient, and secure communications of urgently needed information. Hence, the mechanisms for communicating abnormal test results are not being determined or limited by privacy and security concerns, but rather these mechanisms reflect the most effective and efficient manner of communicating and exchanging information.

## ANALYSIS OF SCENARIO #17 PUBLIC HEALTH - SCENARIO C COUNTY PROGRAMS FOR CHEMICAL DEPENDENCY

---

### SCENARIO OVERVIEW

---

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

To provide structure for the Variation Work Group's discussion and analysis of this scenario, staff identified two key issues and four questions for consideration (see Expanded Scenario #17). The key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario and likely to trigger specific business policies and practices. The identified issues were:

- **Sharing of Drug Treatment Information with County Programs for Reimbursement:** This issue was identified as a key issue to determine if any Minnesota legal requirements mandate the disclosure of individuals' chemical dependency treatment information to counties as part of the payment process for individuals' chemical dependency treatment.
- **Sharing of Drug Treatment Information with Homeless Shelters:** This issue was identified as a key issue to determine any Minnesota legal requirements that need to be satisfied for a drug treatment clinic to report patient-identified treatment data to a homeless shelter.

The four questions for consideration were intended to focus the Work Group's discussion and attempted to:

- Determine what patient-identified information, if any, would be exchanged between a drug treatment clinic and a county social service agency as part of the payment/reimbursement process.
- Investigate any Minnesota requirements or permissions for drug treatment programs to disclose patient-identified data to homeless shelters.
- Examine the mechanisms used to exchange patient-identified data relevant to this scenario.
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

### GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO

---

During the Variations Work Group's discussion of this scenario, it was noted that a number of the scenario's assumptions were at odds with Minnesota's processes for providing chemical health treatment services, specifically:

- When treatment for chemical dependency requires the expenditure of public funds, Minnesota Rules 9530.6600 - 9530.6655 (i.e., Rule 25) require Minnesota counties to provide a chemical use assessment for each client seeking treatment or for whom treatment is sought for chemical dependency problems. This assessment must occur before a client can be placed in a drug treatment program. Hence, the primary care provider would probably not refer the homeless person to a drug treatment program, but rather to the county's social service agency for a chemical use assessment and placement.
- Although Minnesota counties are responsible for conducting a chemical use assessment and determining the appropriate level of treatment for individuals needing chemical dependency treatment services, the drug treatment center is paid through the Minnesota Department of Human Services' usual health care claims process.
- Minnesota law does not require drug treatment centers to report patient-identified drug treatment information to homeless shelters.

The following discussion addresses the general process for placing a homeless person in a chemical dependency treatment program.

#### **Exchange of Individual-Identified Data during Assessment**

Minnesota law makes county social service agencies responsible for the provision of chemical use assessments to every county resident who requests one, or for whom one is requested. Chemical use assessments, also known as Rule 25 assessments, use uniform statewide assessment and placement criteria for rating chemical involvement in an individual's life, determining the appropriateness of treatment, and selecting the appropriate type and intensity of treatment.

At the start of an individual's chemical use assessment, staff is required to obtain the individual's authorization to obtain additional information necessary to complete the chemical use assessment. This additional information may include diagnostic test results, review of relevant medical, legal, mental health and previous treatment records, a physical screening results, and interviews with other people in that individual's life.

Staff is also required to obtain the individual's authorization to exchange necessary treatment plan information with the Minnesota Department of Human Services and the drug treatment center where the individual will be placed in treatment. Hence, counties may only request or disclose information related to the chemical use assessment and placement process with individuals' written authorization, which is obtained at the start of the assessment process.

#### **Exchange of Individual-Identified Data after Assessment**

After a chemical use assessment has determined the appropriate level of treatment, counties enter their client placement authorization data in the Minnesota Department of Human Services' Medicaid Management Information System (MMIS). Once the individual's information and placement authorization is entered into the system, the Department of Human Services is responsible for generating letters to the individual and the drug treatment center indicating that payment has been approved for the individual's treatment. In the case of a homeless person, the letter approving payment for treatment is usually sent to the county staff working with the homeless individual.

Once the individual and drug treatment program have been notified that payment has been approved for treatment, it is the individual's responsibility to contact the drug treatment program and begin care. Although payment is not officially approved until the drug treatment program receives notification from DHS, it is not uncommon for counties to fax placement information directly to drug treatment programs alerting

them to watch for the notification approving payment. As stated previously, the county's disclosure of placement information to the drug treatment program is only permitted with the patient's authorization.

In general, drug treatment centers report very little individually-identified information back to counties on individuals' treatment. The only patient-identified information drug treatment programs usually report to counties is:

- The date the client starts treatment;
- The date the client ends treatment; and
- Information necessary to request a change in the approved treatment placement when the treatment program believes the approved treatment is not adequate.

The exchange of individually-identified information for billing activities is done through the normal health care claims process with DHS. Prior to providing services, the drug treatment center requires the individual to sign an authorization permitting the treatment center to provide the Department of Human Services the information necessary to process its claims.

**Disclosing Individual-Identified Health Data to Others**

When a homeless person enters chemical dependency treatment he is provided the same privacy rights as any other person seeking treatment regardless of payment source. Therefore, drug treatment programs are generally prohibited from disclosing patient-identified health information without the patient's written consent under both federal and state law (42 CFR Part 2 and Minnesota Statutes § 144.335).

The disclosure of any information to a homeless shelter about the homeless person's participation in a drug treatment program, including that the individual is even in treatment, requires the individual's written consent. Similarly, the disclosure of any information to the homeless person's relatives also requires the individual's written consent.

Any treatment information supplied to the county regarding an individual's treatment must be consistent with the individual's written consent obtained during the assessment process, although counties generally do not requested detailed treatment data.

**Impact of Key Issues**

**Sharing of Drug Treatment Information with County Programs for Reimbursement:** In Minnesota, counties are responsible for conducting chemical use assessments and placements for individuals seeking chemical dependency treatment. Any information requested or disclosed during the assessment process is done with the client's written authorization. Beyond authorizing treatment services, counties are not responsible for processing payments to drug treatment centers. The Department of Human Services is responsible for paying drug treatment programs for services rendered and carries out its responsibilities through its normal Medicaid claims processing system. Any information exchanged through the payment process is also done with the client's written consent, which was obtained at the start of the treatment program.

**Sharing of Drug Treatment Information with Homeless Shelters:** Drug treatment programs are generally prohibited under both federal and state law from disclosing patient-identified health information without the patient's written consent. Any treatment or health information disclosed to a homeless shelter, family members, or others is disclosed with the patient's written consent.

### **Variations in Business Practice**

The discussion and analysis of this scenario did not reveal any significant variations in Minnesota counties' processes for conducting chemical use assessments and placements in chemical dependency treatment programs. Minnesota uses uniform, statewide assessment and placement criteria so the lack of significant variation is not surprising. Similarly, the claims payment process for drug treatment providers' services is centralized at the Department of Human Services and is handled in a uniform fashion for all counties.

The discussion did not identify any significant variations in how drug treatment providers disclose patient-identified data. All treatment providers reported following federal and state laws requiring the patient's written consent to release any patient-identified information.

---

## **APPLICATION OF THE PROJECT PRIVACY AND SECURITY DOMAINS**

---

Variation Work Group members were asked to consider the intersection between the project's nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario. No additional issues were identified.

---

## **IDENTIFIED BARRIERS OR BEST PRACTICES**

---

The discussion of this scenario did not identify any privacy or security barriers to the appropriate exchange of information within this scenario. Patient consent and authorization is the most significant privacy requirement that must be satisfied for the exchange of individually-identified health information within the scenario. Federal and state law requires counties, DHS, and chemical dependency treatment providers to obtain the patient's consent prior to disclosing any individually identified health information related to chemical dependency. Consequently, all entities involved in an individual's chemical dependency assessment, placement, and treatment have policies and business practices for obtaining and documenting the patient's written consent before disclosing patient-identified information.

## ANALYSIS OF SCENARIO #18 HEALTH OVERSIGHT LEGAL COMPLIANCE/GOVERNMENT ACCOUNTABILITY

---

### SCENARIO OVERVIEW

---

*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. 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.*

To provide structure for the discussion and analysis of this scenario, staff identified three key issues and six questions for consideration (see Expanded Scenario #18). The key issues identified were the aspects of the scenario that were anticipated to be most significant to the scenario and likely to trigger specific business policies and practices. The identified issues were:

- **Sharing Individual-Identifiable Immunization and Lead Screening Data across State Agencies:** This issue was a key issue because many public health programs have unique data privacy requirements for the use and disclosure of their data. We anticipated that Minnesota's Immunization Registry and Blood Lead Surveillance System have specific statutory requirements for the use and disclosure of individual-identifiable health information.
- **Collection and Use of Individual-Identifiable Data from Electronic Health Records and Registries for Assessing Health Care Quality:** This issue was identified as a key issue because most public health programs are created to address particular public health needs. Many programs' authority to use and disclose data is often limited to particular public health activities. Therefore, we wanted to determine if assessing health care quality is consistent with the statutory authorities of the programs with immunization and lead screening data.
- **Facilitation of Two-Way, Electronic Communication and Exchanges of Information Between Public and Private Sector Entities with Responsibilities Related to Immunizations and Lead Screening:** This issue was identified as a key issue to find privacy/security concerns that inhibit the electronic exchange of information between public and private sector entities responsible for ensuring that children receive appropriate healthcare.

The six questions for consideration were intended to focus the discussion and attempted to:

- Determine state agencies' data privacy limitations/concerns with sharing individual-identifiable health information with other state agencies.
- Identify any anticipated difficulties linking individual-identifiable data from multiple state agencies.
- Investigate state agencies' data privacy limitations/concerns with providing individual-identifiable health information for ongoing analysis.

- Determine if health care providers' electronic health records contain information useful for addressing the quality assessment task of this scenario.
- Assess if state agencies would have privacy/security concerns about being able to access information in health care providers' electronic health records.
- Describe the intersection of the scenario with the nine privacy and security domains used within the project.

---

### **GENERAL BUSINESS PROCESSES IN ADDRESSING THE SCENARIO**

---

We analyzed this scenario with the state agencies involved in children's health care that are most likely to have data related to the quality assessment task. We included:

- The Minnesota Department of Human Services (DHS), which is Minnesota's Medicaid Agency. DHS maintains the Medicaid enrollment files, which identify those children enrolled in Medicaid. It also maintains Medicaid claims data, which identify the services provided and paid for under the Medicaid program.
- The Minnesota Department of Health, which is responsible for Minnesota's Immunization Registry and the Blood Lead Surveillance System. The Immunization Registry is a statewide registry that contains children's immunization records. The Blood Lead Surveillance System contains all blood lead analyses for Minnesota residents as reported by laboratories.

The scenario asks the state agencies to contribute data to the state university. In Minnesota, both DHS and MDH have sufficient expertise, experience, and resources to complete the quality assessment task. In fact, some aspects of this scenario are already being done by DHS and MDH. It is extremely unlikely that the state university would do this task on behalf of the agencies. We therefore eliminated this aspect of the scenario.

#### **Disclosure of Medicaid Data**

In general and without other legal authority, DHS may not disclose individual-identifiable information about persons enrolled in Minnesota's Medicaid program unless the disclosure is essential for the administration of the program. This prohibition also includes communicating the fact that a person is enrolled in the Medicaid program.

To disclose individual-identifiable data as required for the activities of this scenario, DHS would need to make a number of determinations. First, DHS would want to clearly understand the purpose of the activities and how the data will be used. The project would then be evaluated to determine if it was essential for the administration of the Medicaid program. Although DHS would need more detail than is presented in this short scenario, it was generally believed that the proposed tasks would be consistent with its authority to disclose data. However depending on the details, DHS may need to consult with the Centers for Medicare and Medicaid Services.

The second determination DHS would make is whether or not the project is consistent with the combined enrollment/consent forms that Medicaid enrollees sign at enrollment. While it was believed that the project would be consistent, it would need to be verified.

#### **Disclosure of Blood Lead Surveillance System Data**

The Blood Lead Surveillance System's authority to share individual-identifiable data is very limited. Minnesota Statutes § 144.9502, Subd. 9 restricts MDH's authority to disclose these data to the Minnesota Department of Labor and Industry, authorized agents of Indian Tribes, and local boards of health. The same

section of Statutes also restricts all of the entities' uses of individual-identified data to the purposes set forth in the Statutes.

Although MDH would want more details about the project proposed within the scenario, it was generally believed that the activities would be consistent with the Blood Lead Surveillance System's statutory authorities for using the data collected. It should be noted that MDH does not have the authority to disclose individual-identifiable blood lead data to DHS. Consequently, the tasks and analyses proposed by this scenario would almost certainly need to be performed by MDH.

#### **Disclose of Immunization Registry Data**

The Minnesota Immunization Registry has authority (Minnesota Statutes § 144.3351) to disclose individual-identifiable immunization data to health care providers, health plans, schools, local boards of health, and others. Under this authority, immunization data may be disclosed to DHS, the state Medicaid Agency. Similarly, immunization data could be used internally by MDH to conduct the activities and analyses proposed in this scenario.

#### **Centralization of Data from All Sources**

This scenario calls for individual-identifiable data from four sources (i.e., Medicaid enrollment files, Medicaid Claims, Blood Lead Surveillance System, and Minnesota Immunization Registry) to be centralized into one information system for analysis. Given the legal requirements and data privacy constraints of the four data sources, data centralization and analysis could only be done at MDH.

Some portions of the proposed analyses are already being done in Minnesota. DHS has provided Medicaid data to MDH's Blood Lead Surveillance System to permit the two agencies to follow trends in lead testing and blood lead levels for children enrolled in Medicaid, to track outcomes associated with blood lead testing and follow-up care, and to monitor the completeness of lead test reporting by state laboratories. Similarly, the Minnesota Immunization Registry and DHS have exchanged data. The Immunization Registry has provided immunization data to DHS to assist in calculating HEDIS measures and DHS has provided data to the registry to populate the registry with immunization data available in DHS' administrative data and missing from the registry.

This scenario also calls for on-going data exchange and analysis. It is unclear if the on-going exchange means providing periodic snapshots of data (e.g., annual) or connecting the data sources to allow real-time analysis. As mentioned above, the first type of on-going exchange already occurs. The second type of on-going exchange would be unnecessary for producing annual reports on the quality of children's healthcare. The benefit from connecting data sources and enabling real-time data exchange would be the ability to impact health care providers' actions.

One way that a real-time system could impact providers' actions is by supplying providers with up-to-date information about the children being seen. For example, all children enrolled in Medicaid should be tested for elevated blood lead levels at 12 and 24 months of age. Ideally, DHS would provide enrollment data to the Blood Lead Surveillance System to identify children not yet tested. Then, the Surveillance System would supply data that identifies children needing a blood lead screening test or follow-up for elevated blood lead levels to the Immunization Registry. This exchange would permit the Immunization Registry to flag the immunization records of children needing blood lead screening services. This flagged record would then alert the provider of the need to conduct or follow-up on a blood lead screening.

While such a real-time system would be useful in alerting health care providers to children's healthcare needs, it raises a number of data privacy concerns. First, it would indirectly disclose children's Medicaid enrollment status to all who have access to the Immunization Registry, because only children enrolled in Medicaid are automatically considered high risk for elevated blood lead levels and are required to be screened. Identifying Medicaid enrollees in this manner is not permitted. Similarly, MDH does not have

statutory authority to share blood lead level data with physicians or others with access to the Immunization Registry. Consequently, the most useful benefits from exchanging data in real-time are not permitted under the authority of the various programs.

#### **Linking of Individual-Identifiable Data**

Both DHS and MDH are familiar with the difficulty of linking information from the four data sources. In previous projects, the agencies linked Medicaid data with the Surveillance System data using first name, last name, date of birth, and gender. The process for linking used a seven step iterative process that was adapted from previous research linking Medicaid claims data to Minnesota's vital records data:

- **Iteration 1:** Exact last and first name, and exact month, day, and year of birth.
- **Iteration 2:** Index function on last and first names, and exact month, day, and year of birth.
- **Iteration 3:** Index function on last and first names, gender, exact month, and year of birth.
- **Iteration 4:** Index function on last and first names, gender, exact day, and year of birth.
- **Iteration 5:** 'Sounds like' operator on matching last name, first name, exact day, month, and year of birth.
- **Iteration 6:** 'Sounds like' operator on matching last name, first name, exact day, and year of birth.
- **Iteration 7:** 'Sounds like' operator on matching last name, first name, exact month, and year of birth.

This matching process is not perfect. A unique personal identifier common to both data sets would greatly facilitate the linking process; however, the iterative process is sufficient to allow data analysis.

The Immunization Registry also has considerable experience in matching records and people. Operating the Registry requires that children are appropriately matched to their records. Although the Immunization Registry does not use a unique identifier to match people with their immunization records, it has additional fields to use in the linking process, including: Mother's first name, mother's maiden name, and address.

Although these data sources can be linked without a unique personal identifier, the quality and completeness of the linkage is dependent on the demographic fields available in the data sources. All of these programs agreed that matching records across data sources and linking individuals to records would be more complete and accurate if a unique personal identifier were available and used.

#### **Accessing Data Directly from an Electronic Health Record**

The information contained in Medicaid claims, the Blood Lead Surveillance System and the Immunization Registry is generally a subset of the data contained in health care providers' electronic health records. Therefore, we asked DHS and MDH if there are data in providers' electronic health records useful for completing the task proposed by this scenario. We also asked the programs if they would have privacy/security concerns about being able to access such information directly.

The Medicaid program agreed that health care providers' medical records are more complete than claims data and could aid in assessing the appropriateness and adequacy of children's health care. Additionally, the Medicaid program currently has authority to access any data related to services paid for by the Medicaid program. The current process for accessing such data involves the expensive and time-consuming process of manual chart review. Therefore, the ability to access such information electronically would be a tremendous benefit for collecting quality assessment data.

The greatest concern of the Medicaid program with the ability to access providers' electronic health records is the capacity to limit the access to only data related to services paid for under the Medicaid program. That is, an electronic health record contains a great deal of information about an individual's health care that was not paid for by Medicaid, and DHS does not have authority to collect these data. The same concern exists today when DHS does manual chart reviews, where data recorded by chart auditors is limited to Medicaid covered services.

The Blood Lead Surveillance System believed that access to providers' electronic health records would greatly facilitate the Surveillance System's ability to follow-up on cases of elevated blood lead levels. When a child's lead screening test shows an elevated blood lead level, it would be helpful to know if the child was receiving treatment. Access to electronic health records would speed the Surveillance System's capacity to know when a child received follow-up testing and when the blood lead levels returned to normal.

The Surveillance System was also concerned that any such access would need to be limited to lead screening data. It was also noted that the Surveillance System may have sufficient authority to collect such data, but it does not have authority to disclose information back to providers.

The Immunization Registry agreed that the ability to exchange information with providers' electronic health records could improve the completeness of both the Registry and providers' records. Direct exchange between the Registry and providers' electronic health records would allow providers to fill gaps in their health records more completely and accurately. The Immunization Registry would be able to document situations where immunization is unnecessary. For example, access to the medical history portion of electronic health records would allow the Immunization Registry to document when a person has had chicken pox and consequently, would not need a varicella vaccine.

The Immunization Registry also would like to have a more direct connection with electronic health records to facilitate the current exchange of information. Today, providers need to leave their organization's electronic health record and open a web browser to access the Immunization Registry. The need to switch computer programs to access immunization data is functional, but cumbersome. Ideally, the provider would be able to access the information from within the electronic health record and the process would be seamlessly integrated into the normal workflow.

### **Impact of Key Issues**

**Sharing Individual-Identifiable Immunization and Lead Screening Data across State Agencies:** The main data sources related to this scenario are Medicaid enrollment and claims, the Blood Lead Surveillance System, and the Minnesota Immunization Registry. Each of the data sources has unique legal authority for using and disclosing data. The quality assessment task proposed by this scenario would probably be possible under the existing authorities as it is similar to existing DHS and MDH projects. The Blood Lead Surveillance System has the most restrictive authorities related to disclosing individual-identifiable data and would require that the scenario activities be done at MDH.

**Collection and Use of Individual-Identifiable Data from Electronic Health Records and Registries for Assessing Health Care Quality:** The Medicaid program has legal authority to access health records for services paid for by the program. The Immunization Registry has authority to exchange immunization information with providers. The Blood Lead Surveillance System has authority to collect blood lead level data. If the appropriate information were available electronically through electronic health records, the programs would be permitted and willing to access it. However, all of the programs were concerned that any such access would need to be appropriately restricted to only data for which the programs have authority.

**Facilitation of Two-Way, Electronic Communication and Exchanges of Information Between Public and Private Sector Entities with Responsibilities Related to Immunizations and Lead Screening:** The two-way exchange of information between health care providers and the three programs with data related to this scenario is complicated. The Immunization Registry has the broadest authority to share data

and is able to disclose immunization data to providers. The Blood Lead Surveillance System does not have authority to disclose information to providers and would be prohibited from a two-way exchange of information. The Medicaid program has authority to disclose data, but must look at the specific purposes and mechanisms for disclosing data in order to determine the appropriateness and legality of two-way exchanges.

**Application of the Project Privacy and Security Domains**

The Medicaid Program, the Blood Lead Surveillance System and the Immunization Registry were asked to consider the intersection between the project’s nine privacy and security domains and the scenario to identify any additional issues relevant to the discussion of the scenario.

**State Law Restrictions**

The Immunization Registry identified a significant barrier to the collection and disclosure of immunization data. In general, Minnesota Statutes § 144.335, Subd. 3a restricts the disclosure of patients’ health records without patients’ written consent. Minnesota Statutes § 144.3351 provides the Minnesota Immunization Registry authority to share immunization data without patient consent and details the individuals and entities that may exchange information. This section of the Statutes is intended to serve two purposes: 1) permit the appropriate exchange of immunization data without patient consent; and 2) limit those individuals and entities with whom data may be exchanged.

While Minnesota Statutes §144.3351 authorizes providers to exchange immunization data without patient consent, the definition of provider limits the exchange to health care providers licensed/registered in Minnesota. Consequently, the Immunization Registry is unable to exchange immunization data with health care providers licensed outside of Minnesota. This limitation makes it very difficult to maintain complete and accurate immunization records for children living near the state border and receiving care on both sides of the border.

Drawing boundaries and limiting which individuals/entities may exchange immunization data without consent was done to protect individuals’ privacy. However, the definition of provider used in Minnesota Statutes limits the utility of the Immunization Registry and makes it impossible to exchange immunization data with border-state providers. The definition of provider leads to a portion of the Registry being incomplete without adding any clearly identifiable privacy protections.

---

**IDENTIFIED BARRIERS OR BEST PRACTICES**

---

The most significant barrier to the appropriate exchange of information identified during the analysis of this scenario is not directly related to the scenario’s main task. Rather, the most significant barrier is the Immunization Registry’s statutory restrictions for exchanging immunization data with health care providers not licensed in Minnesota. Minnesota Statutes permit the exchange of immunization data with health care providers, but restricts the definition of providers to Minnesota-licensed providers. The consequence of this definitional restriction is that some immunization records are incomplete, particularly for children living near the state border and receiving health care on both sides of the border.

A second issue identified as a serious limitation in executing the activities proposed in the scenario is the Blood Lead Surveillance System’s authority to disclose individual-identifiable data. The Surveillance System is statutorily restricted to sharing individual-identifiable data to Minnesota Department of Labor and Industry, authorized agents of Indian Tribes, and local boards of health. Consequently, the quality assessment activities proposed in this scenario could only be done by the Minnesota Department of Health. Although this is not a barrier to completing the task, it does significantly limit how the task may be done.