

Security and Privacy Solutions for Interoperable Health Information Exchange

Interim Assessment of Variations Report

Subcontract No.
RTI Project No. 9825

Prepared by:

Wisconsin Department of Health and Family Services
Division of Public Health
1 West Wilson Street, Room 372
Madison, WI 53702

in partnership with
UW School of Medicine and Public Health, Population Health Institute

Submitted to:

Linda Dimitropoulos, Project Director
Security and Privacy Solutions for
Interoperable Health Information Exchange

Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

November 11, 2006



Table of Contents

Executive Summary	3
1. Methodology Section	6
Variations Workgroup	6
Legal Workgroup	7
2. Summary of Relevant Findings Purposes for Information Exchange	9
2.1 Treatment (Scenarios 1–4).....	9
2.1.1 Stakeholders.....	9
2.1.2 Summary of Findings.....	9
2.1.3 Domains.....	15
2.1.4 Critical Observations.....	21
2.2 Payment (Scenario 5).....	23
2.2.1 Stakeholders.....	23
2.2.2 Summary of Findings.....	23
2.2.3 Domains.....	24
2.2.4 Critical Observations.....	26
2.3 RHIO (Scenario 6).....	28
2.4. Research (Scenario 7).....	29
2.4.1 Stakeholders.....	29
2.4.2 Summary of Findings.....	29
2.4.3 Domains.....	30
2.4.4 Critical Observations.....	31
2.5 Law Enforcement (Scenario 8).....	33
2.5.1 Stakeholders.....	33
2.5.2 Summary of Findings.....	33
2.5.3 Domains.....	34
2.5.4 Critical Observations.....	36
2.6 Prescription Drug Use/Benefit (Scenarios 9 and 10).....	38
2.6.1 Stakeholders.....	38
Summary of Findings.....	38
2.6.3 Domains.....	40
2.6.4 Critical Observations.....	43
2.7 Healthcare Operations/Marketing (Scenarios 11 and 12).....	44
2.7.1 Stakeholders.....	44
2.7.2 Summary of Findings.....	44
2.7.3 Domains.....	47
2.7.4 Critical Observations.....	50

2.8. Public Health/Bioterrorism (Scenario 13)	52
2.8.1 Stakeholders	52
2.8.2 Summary of Findings.....	52
2.8.3 Domains	54
2.8.4 Critical Observations	58
2.9. Employee Health (Scenario 14)	60
2.9.1 Stakeholders	60
2.9.2 Summary of Findings.....	60
2.9.3 Domains	61
2.9.4 Critical Observations	63
2.10. Public Health (Scenarios 15–17)	64
2.10.1 Stakeholders	64
2.10.2 Summary of Findings.....	64
2.10.3 Domains	70
2.10.4 Critical Observations	76
2.11. State Government Oversight (Scenario 18)	64
2.11.1 Stakeholders	79
2.11.2 Summary of Findings.....	79
2.11.3 Domains	80
2.11.4 Critical Observations	82
3. Summary of Critical Observations and Key Issues	84
4. Appendices	90

Executive Summary

The Wisconsin Security and Privacy Team has completed the first phase of work. The first phase consisted of two workgroups, Variations and Legal, who reviewed eighteen scenarios designed by RTI to highlight potential issues related to health information exchange (HIE).

Methods

The Variations Workgroup was comprised of security and privacy experts from sixteen different organizations, selected to meet the stakeholder requirements developed by RTI. The workgroup held four sessions to discuss business practices associated with each scenario. The results of the workgroup are documentation of detailed variations in business practices associated with the scenarios, as well as determination of the driver of each business practice and which practices pose barriers to HIE.

The Legal Workgroup was comprised of fifteen security and privacy law experts from various organizations across Wisconsin. The Legal Workgroup analyzed each scenario as well as the variations in business practices described by the Variations Workgroup to identify legal barriers to HIE and determine which Variations Workgroup barriers are driven by law versus business practice or policy.

The Interim Assessment of Variations Report contains the results of the Variations and Legal Workgroups' analysis. A Solutions Workgroup is now being assembled to review the barriers to HIE as determined by the Variations and Legal Workgroups and develop solutions to the barriers while maintaining security and privacy standards. An Implementation Workgroup will then convene to determine how to implement the outlined solutions.

The scenarios analyzed by the Variations and Legal Workgroups were designed by RTI to highlight potential issues related to HIE. The exchanges in the scenarios covered the following realms:

- Treatment
- Payment
- RHIO
- Research
- Law Enforcement
- Prescription Drug Use/Benefit
- Healthcare Operations/Marketing
- Bioterrorism
- Employee Health
- Public Health
- State Government Oversight

Business practices and laws governing practices were to be analyzed in the following domains:

- User and entity authentication
- Information authorization and access controls
- Patient and provider identification
- Information transmission security or exchange protocols
- Information protection (against improper modification)
- Information audits that record and monitor activity
- Administrative or physical security safeguards

- State law restrictions
- Information use and disclosure policy

Results

The Variations and Legal Workgroups found several barriers to HIE that are driven by laws, policies, and practices. The barriers are summarized below:

Barriers driven by Wisconsin state law

Wisconsin statutory requirements that are more restrictive than federal requirements cause barriers to the exchange of information.

Some of the greatest barriers to HIE are the regulations associated with the treatment of sensitive information, defined as information pertaining to mental health, alcohol and drug abuse and developmentally disabled. The requirements include:

- Consent for all disclosures (payment and treatment)
- Verification of the requestor for this information
- Additional documentation of these disclosures

HIV test results are also treated as sensitive information, except that they can be disclosed from provider to provider for treatment purposes.

Other barriers driven by Wisconsin state law include:

- Documentation of all disclosures made with or without patient consent
- Requirements prohibiting re-disclosure of health information

Barriers driven by state and federal law

The greatest hurdles to exchange that are governed by state and federal law are the consent requirements. The barriers are caused by:

- The process to obtain a consent, including determination of who is able to sign
- Validation of the statutorily required elements of the consent
- Interface between state and federal law to determine which law controls
- Variation between states in requirements

Barriers driven by federal law

In some cases, we found that federal law is more stringent than state law. In all of these cases, both the law and the varying interpretations of the law cause barriers to exchange. The federal requirements that the workgroups felt pose barriers to exchange include:

- Verification of requester
- Minimum necessary
- Business associate agreements
- Federal Privacy Rule

Barriers driven by policies and practices

The Variations and Legal Workgroups identified several barriers to HIE that are driven policies and practices. Most often it is the variation in how these processes are performed that lead to barriers to HIE.

Barriers driven by policies and practices include:

- Consent – varying interpretations of when consent is required for disclosure
- Method of requesting information – varying methods for making requests
- Method of disclosure – varying methods for disclosing information

The final barrier to exchange identified by the workgroups is technology. Current technology cannot limit access to relevant parts of the record or to specific records to comply with minimum necessary requirements. Furthermore, current technology cannot often specify the type of access (read-only, edit/modify, delete) granted to the user. For those who do not have electronic medical records, the lack of technology creates a barrier to exchange.

Opportunities

The Variations and Legal Workgroups see many opportunities for solutions to the barriers to HIE and are looking forward to the results of the Solutions and Implementation Workgroups.

While many barriers are driven by variations in business practice, we feel that the Solutions Workgroup should focus on changes in the law and technological advances to remove barriers to HIE while paying attention to the security and privacy rights the current practices are preserving. Attention should also be given to developing solutions to achieve best practices and develop policies that regulate information exchange. Model practices designed to achieve a balance that encourages and enhances best patient care practices with privacy protections should be developed. In some cases, the barriers exist to protect patient information and should not be removed. In other cases, removing the barriers would improve patient care.

We believe the workgroup should first focus on areas where state and federal law differ and make recommendations as to which law should be followed. With technology, the Solutions Workgroup should look at improvements to existing technology as well as a plan for wider adoption of electronic medical records.

1. Methodology Section

Methodology

Wisconsin's Department of Health and Family Services (DHFS) was awarded a contract by RTI International, Inc. (RTI) to participate in the Health Information Security and Privacy Collaboration (HISPC), to be referred to as the Security and Privacy Project throughout the report. This project is part of a national effort to collect and analyze data from the participating state to identify variations in organizational business practices, policies and laws related to the exchange of health information.

The Security and Privacy Project coincides with Governor Doyle's eHealth Initiative to develop a statewide plan for the adoption and implementation of the exchange of electronic health information. The eHealth Initiative began with Governor Doyle's November 2005 Executive Order to create the eHealth Care Quality and Patient Safety Board (eHealth Board). The eHealth Board serves as the Steering Committee for the Security and Privacy Project and will be informed by the project results as an exchange is developed in Wisconsin.

The Security and Privacy Team includes staff of the Wisconsin Department of Health and Family Services and contractors who are serving as project management. The Security and Privacy Team is responsible for managing the process, identifying key stakeholders for participation in the workgroups, and documenting business policies and practices.

Variations Workgroup

Membership

Wisconsin's Variations Workgroup was developed to have one representative for each stakeholder group required through the grant. DHFS reached out to numerous leaders within the community, resulting in a wide range of experience and expertise. The Consumer role was filled by two members currently serving as appointed representatives to the Governor's eHealth Consumer Interests Workgroup.

The Variations Workgroup included 16 members representing the following stakeholder groups:

- Clinicians
- Community Clinics and health centers
- Consumer
- Correctional Facilities
- Federal Health Facility
- Home Care and Hospice Care
- Hospitals
- Laboratories
- Long Term Care Facilities and Nursing Homes
- Medical and Public Health Schools
- Payers
- Pharmacies
- Physician Groups - Large
- Physician Groups - Small
- Professional Organizations and Societies
- Public Health Agencies
- Quality Improvement Organizations
- State Government

The Variations Workgroup was chaired by Chrisann Lemery, RHIA, a member of the Governor's eHealth Initiative Consumer Interests Workgroup and the Security Officer for WEA Trust.

Process

DHFS asked all the Variations Workgroup members to be present or send a replacement representative for all the meetings. This was done to ensure that none of the stakeholder groups were overlooked in their representative role in a scenario or as an observer with expertise that would be valuable to the identification of business practices.

The Variations Workgroup held four five-hour sessions in which the stakeholders reviewed the scenarios provided by RTI. Each scenario was initially read to the group, initial assumptions identified, and potential barriers to exchange highlighted for the group to consider. The Workgroup identified business practices and policies related to the scenarios provided by RTI and determined which practices were barriers to HIE. Each scenario was evaluated in terms of the nine domains of security and privacy provided by RTI. The Security and Privacy Team developed a structured methodology for collecting from the workgroup members the business policies and practices, assumptions, and the reason for the business practice identified. The Security and Privacy Team was responsible for recording this information, assigning the domain, and assisting in identification of barriers based on the discussion and on the definition provided by RTI.

Following the first meeting, the team met to re-evaluate and refine the process to ensure that all relevant information was being collected. Although the format for collecting this information was very structured, the workgroup was provided opportunities for identifying the most cumbersome and/or restrictive practices, policies, and laws in exchanging health information.

Following each scenario, workgroup members were asked to respond to the scenario as a consumer. They were asked to identify if the process that was described was what they expected to occur and whether this information changed their views of the process.

The final meeting was scheduled for the purpose of final review and filling any gaps that may have been observed by the team. At this meeting, a high level summary of the business practices identified was provided for the group to review. This document highlighted in a non-specific format where variations in practice, policy, or law were observed.

Legal Workgroup

The Legal Workgroup conducted three meetings and will be reviewing and completing their work at a final meeting scheduled in November. The Group was chaired by Chrisann Lemery, RHIA, who also chaired the Variations Workgroup enhancing continuity across these groups. Ms. Lemery has also served as Co-Chair of the HIPAA Collaborative of Wisconsin (COW) Privacy Workgroup and this group recently completed an analysis of interface between state and federal privacy laws for this group. This is a non-profit organization open to entities considered to be Covered Entities, Business

Associates, and/or Trading Partners under HIPAA, as well as any other organization impacted by HIPAA regulation

The purpose of the Legal Workgroup was to identify the legal drivers for the business practices identified by the Variations Workgroup. This workgroup was charged with analyzing variations in security and privacy business policies and practices and mapping relevant policies and practices to state and federal law to determine which laws pose barriers to health information exchange (HIE). The Workgroup was also charged with analyzing the business practices presented and determining the laws and/or regulations that apply to the scenarios and the identified business practices.

The Legal Workgroup was comprised of 15 members from the Security and Privacy Workgroup of Wisconsin's HIPAA Collaborative of Wisconsin. The members on this workgroup represented the following stakeholders:

- Hospitals
- Clinicians
- Consumers
- Physician Groups
- Payers
- Public Health Agencies
- Quality Improvement Organizations
- State Government

In an effort to simplify the process, the Security and Privacy Team prepared a core set of practices for each scenario. This core set of business practices was used to identify the state and federal legal drivers for each of those practices. Lack of a legal driver was also noted when appropriate.

The legal drivers and federal or state statutory references related to each scenario were identified, discussed and documented. The Legal Workgroup conducted a detailed legal review of each scenario, outlined the applicable state and federal laws and the barriers presented by law, policy or business practice. The workgroup was asked to identify whether the legal drivers currently identified presented a barrier to exchange of health information in both a paper and electronic environment. Some of the members of this workgroup are already in environments where electronic health records are used, and therefore could provide some insight into barriers that have already been observed. The Legal Workgroup also discussed possible practice and legal solutions to identified barriers. Upon completion of the review by the Legal Workgroup, the Privacy Consultant reviewed the Workgroup input and wrote the legal analysis.

2. Summary of Relevant Findings-Purposes for Information Exchange

2.1 Treatment (Scenarios 1–4)

The Variations and Legal Workgroups were given 4 treatment scenarios to analyze in order to find variations in current business practices, the legal drivers of the business practice and potential barriers to the exchange of health information.

2.1.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the treatment scenarios:

- Clinicians
- Consumers or consumer organizations
- Federal health facilities
- Homecare and hospice
- Hospitals
- Long term care facilities and nursing homes
- Physician groups
- Professional associations and societies

Please refer to section 1 for a detailed description of the stakeholders.

2.1.2 Summary of Findings

This section contains each scenario followed by the high level findings of the Variations and Legal Workgroups.

Scenario 1 – Patient Care Scenario A

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

Our team assumed that the information requested did not include mental health information.

Variations Workgroup Summary

All relevant workgroup stakeholders would exchange the information (from the previous inpatient stay to the emergency room physician) without patient consent. They would verify the requester (verification processes vary) before processing the request (processes vary). The stakeholders used a variety of methods for making the request and sending the patient

information, including phone, fax and mail. Each would limit the information disclosed to the minimum necessary, but what is deemed necessary varies between workgroup members. This is interesting in that neither state nor federal law requires the application of the minimum necessary restriction records released for treatment.

Legal Analysis

A written authorization is not required under state or federal law¹ to exchange patient information between providers for treatment purposes unless the inpatient information includes specifically protected information such as for mental illness. The Federal Privacy Rule, 45 CFR §§164.502(a) (1) (ii) and 164.506(c) (2), authorizes the use and disclosure of protected health information for treatment without the written or oral consent of the patient. There are two Wisconsin laws that are relevant to this scenario. Wis. Stats. 146.81-146.84² and 51.30³. Wisconsin Statutes 146.81-146.82 govern general healthcare information and contain an exception that allows for release of patient care information from provider to provider for patient treatment. This state law is consistent with the Federal Privacy Rule that also does not require patient consent for disclosure from provider to provider for treatment and consent would not be required.⁴

If the information requested from the out-of-state clinic relating to the anti-psychotic drug was deemed “sensitive” under Wisconsin law (e.g. relating to mental illness, developmentally disabled, alcohol and drug abuse), a specific, written patient consent is required to perform the health information exchange. While HIPAA would normally preempt a contrary state law, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. Consequently, Wisconsin law regulating mental health records would be controlling in this scenario if the information requested contains mental health, alcohol and drug abuse or developmentally disabled information, and consent would be required. If consent is required there are very specific requirements that must be included in the consent form for it to be deemed legal.⁵

Federal law also requires that the identity of the requestor be verified. In this scenario, most of the stakeholders would have verified the identity of the requestor.

Federal law also applies a minimum necessary standard to the amount of information disclosed. However HIPAA does not require that standard be applied when the exchange is for treatment.

This scenario contemplated an exchange of information between providers in two different states. Accordingly, the legal analysis above could be different depending on the law of the unnamed state.

Scenario 2 – Patient Care Scenario B

¹ Wisconsin Statute 146.82(2)(a)2; 45 CFR §§164.502(a)(1)(ii) and 164.506(c)(2),

² Wisconsin Statutes 146.81 – 146.84

³ Wisconsin Statute 51.30

⁴ 45 CFR 164.506(c)(2)

⁵ Wisconsin Statute 51.30 (2)

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

Variations Workgroup Summary

There is variability in how this exchange would be handled. The first exchange based on a request from the primary care provider for information from the substance abuse facility would be more stringently protected under Wisconsin law than federal and consent for disclosure between providers for treatment would be required. The Variations workgroup responded with some requiring consent and some sending the patient information without consent, exemplifying a variation in interpretation and compliance with Wisconsin law.

After receipt of the substance abuse information, the primary care provider then sent the patient's general health information along with the substance abuse information to a specialist. Both state and federal law allowed the disclosure of the primary care notes without patient consent and the stakeholders all allowed that disclosure without patient consent. However the re-disclosure for the substance abuse information, prohibited by state law without a patient consent, met with varied responses. One responder had a policy that incorporated the substance abuse information into their record when received, arguably allowing them to re-disclose the substance abuse information as their record and not as a re-disclosure. Other workgroup members would re-disclose the information (obtained from the treatment facility) to the specialist without a consent. Others would require consent to re-disclose information. Again, exemplifying the variability in interpreting the law and applying the law. Of note, is the "work-around" created by one of the stakeholders to allow disclosure between providers for treatment purposes without patient consent when it would appear that state law requires consent. There was also variability in how the information would be sent – some mail, some fax.

Legal Analysis

The stakeholders clearly identified that general healthcare information could be disclosed without patient consent between providers for treatment purposes under both state and federal privacy laws (HIPAA)⁶. The divergence occurred when state and a federal law other than HIPAA, relating to alcohol and drug abuse, required a patient consent for disclosure of information from the substance abuse facility (alcohol and drug abuse treatment information).⁷ This divergence in law then requires interface between state and federal law that is specifically addressed under HIPAA.⁸ The resolution, by federal law, is to apply the law, state or federal that provides the most protection to the patient information. In this scenario, HIPAA would require application of the more stringent requirements under state law and consent from the patient

⁶ Wis. Stat. 146.82(2)(a)2; 45 CFR 164.506

⁷ Wis. Stat. 51.30(2); 42 CFR 2.1

⁸ 45 CFR §160.203(b)

would be required for disclosure of the substance abuse facility information to the primary care provider.

In addition, state⁹ and federal¹⁰ law allow for re-disclosure with patient consent. The same analysis applied above would control the re-disclosure of the substance abuse facility information to the specialist and re-disclosure would be allowed with patient consent.

Scenario 3 – Patient Care Scenario C

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

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

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

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

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

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

Variations Workgroup Summary

The Variations Workgroup members presented variable solutions to sending sensitive information from an inpatient psychiatric unit to a skilled nursing facility, when a patient is being transferred between facilities, including requiring or not requiring patient consent. Wisconsin law requires patient consent for this disclosure, so practice exemplifies variation in interpretation and application of Wisconsin privacy requirements for more stringently protected patient information.

⁹ HFS 92.03(1)(h)

¹⁰ 42 CFR 2.31

All workgroup members would exchange information without patient consent between a physician and their transcription service utilizing a written business agreement which may be an employment contract or a business associate contract.

All work group members would exchange patient information from the patient's physician for services performed at the skilled nursing facility and the skilled nursing facility without patient consent. However, disclosure practices varied if the physician's information included mental health, alcohol and drug abuse or developmentally disabled, even though Wisconsin law requires a patient consent.

The work group members presented variable solutions for disclosure processes for information related to an inpatient psychiatric stay, verification of requestor, methods for information exchange, policies for auditing/documenting disclosures and for integration of received information into the patient record. Again, the stakeholder practices exemplify significant variability in application and implementation of state and federal privacy laws.

There also seemed to be consensus among the stakeholders that the physician should not have been blocked from providing documentation of the patient visit into the skilled nursing facility record. The Wisconsin physician licensing law requires that a physician document patient services. In this scenario the nursing home practice clearly obstructed the exchange of information between the patient's providers.

Legal Analysis

In this scenario there are several exchanges of information between providers and individuals contracting to provide services to providers. The Legal Workgroup stakeholders clearly identified that if the information exchange was between providers for treatment and related to general health information, no consent would be required for disclosure under state and federal law¹¹. If however, the exchange contained information relating to mental illness, substance abuse or developmental disability as in the exchange between the psychiatric inpatient hospital and the skilled nursing facility, a patient consent for exchange would be required by Wisconsin law and possibly the federal law regulating alcohol and drug abuse records.¹² In addition, Wisconsin law requires that patient information be sent with the patient when transferring from an inpatient facility to a nursing home facility.¹³ So the patient records would be required to be sent to the nursing home facility with a patient consent. If information is transferred electronically, there is no controlling Wisconsin law but the Federal Security Rule would require that the transmission be secure.¹⁴ Wisconsin law also requires that the disclosure of the patient health record from the inpatient psychiatric unit be documented.¹⁵

All stakeholders agree that some type of contractual relationship such as employment or a business associate agreement would be required to share information between the provider and the transcription company. Wisconsin law does not control this exchange as it is considered a use, not a disclosure. The Federal Privacy Rule however requires a written agreement between

¹¹ Wis. Stat. 146.82(2) (a) 2. a and b; 45 CFR 164.506(c)(2);

¹² Wis. Stat. 51.30(2); 42 CFR 2.1

¹³ HFS 132, Nursing Home Records

¹⁴ 45 CFR 164 Subpart C

¹⁵ Wis. Stat. 51.30(4)(e)

the physician and the transcription company that meets the federal requirements before exchange can occur.¹⁶ In this case, federal law is more stringent than state law.

The stakeholders generally agreed that they would not require a patient consent for disclosure of the physician's transcription to the nursing home. It does however appear that if the physician's dictation contains mental health information, consent would be required to share between non-network providers.¹⁷

Scenario 4 – Patient Care Scenario D

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

Variations Workgroup Summary

In the first exchange, most relevant workgroup stakeholders would require consent to release sensitive information (HIV test results) from clinic to physician, even though the state and federal laws do not require patient consent. It is interesting that the practice requiring consent implements a standard more restrictive than state and federal law and creates a barrier to information exchange.

In the second exchange, all relevant workgroup members would release non-sensitive information (mammogram) from clinic to Radiologist without consent.

In the third exchange, all would require consent, signed by an authorized person, to release genetic test results to the niece. There was great variation in how organizations would validate the authorized person. This practice exemplifies compliance with state and federal law when requiring consent, but presents variability in application of the legal requirements for verification of consent.

Legal Analysis

The stakeholders generally agreed that a patient consent would be required to disclose a patient's record, containing an HIV test result, from provider to provider for treatment. This practice applies a more stringent standard than state or federal law requires since neither requires a patient consent for this release.¹⁸ This variation in practice that is more stringent than state or federal law presents a barrier to health information exchange.

¹⁶ 45 CFR 164.502(e)(1)

¹⁷ Wis. Stat. 51.30 (2)

¹⁸ Wis. Stat. 252.15(5)(2); Wis. Stat. 146.82(2)(a)2.; 45 CFR §§164.502(a)(1)(ii) and 164.506(c)(2),

The group uniformly agreed that consent would not be required for transfer of the mammography image between providers for treatment.¹⁹ This practice is consistent with state and federal law that does not require consent.

The Legal Workgroup agreed, consistent with state and federal law, that the exchange of the aunt's genetic information from a provider to the niece would require a valid patient consent. There is no applicable state or federal exception that would allow this disclosure without patient consent, therefore consent would be required. The process of obtaining a valid patient consent with the appropriately legally authorized signature for a deceased patient's information was identified as onerous.²⁰

2.1.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 - Patient and provider identification
- 4 - Information transmission security or exchange protocols
- 5 - Information protection (against improper modification)
- 6 - Information audits that record and monitor activity
- 7 - Administrative or physical security safeguards
- 8 - State law restrictions
- 9 - Information use and disclosure policy

1 – User and Entity Authentication

When receiving a request for health information, all relevant stakeholders stated that they would verify the requester prior to disclosing information. Verification practices occur for both sensitive, more stringently protected, and non-sensitive information, but the practices are variable and often more rigorous for sensitive information. Some stakeholders require the requester to fax a request for information on letterhead, others ask for a phone number, verify the phone number, and then call the requester back. If a request for sensitive information comes from a physician, some verify the physician's signature and license number before disclosing information, while physician to physician requests are often not verified in practice. Additionally, for sensitive information, because consent is required to disclose the information, the consent serves as verification of the request.

Verification practices are driven by federal law, which is more stringent than Wisconsin state law. Federal law states that requests need to be verified, but does not state how the verification should occur. Thus there is wide variation in verification practices.

Verification practices are a barrier to health information exchange, particularly for sensitive information. Variation in verification processes across stakeholders increases the barrier.

¹⁹ Wis. Stat. 146.82(2)(a)2.; 45 CFR §§164.502(a)(1)(ii) and 164.506(c)(2),

²⁰ Wis. Stat. 146.81(2) and (5); 45 CFR 165.508

2 - Information authorization and access controls

The treatment scenarios highlighted several discrepancies in information authorization and access controls amongst the stakeholders. Some variation is due to the fact that very few of our stakeholders have electronic medical records. Those that do have varying levels of controls and those that don't do not have the means to control access to health information.

One of our representative organizations has an electronic medical record wherein anyone with access (role based) to medical records can login and access any part of any record. Access to sensitive information is tracked but not limited. Another stakeholder with an electronic medical record limits access to sensitive information based on employee role. Different systems within the organization have varying capabilities to limit access as well as what the user can do to the data in the system. Wherever possible, access is limited based on organizational role.

The facilities with paper records have no way to limit access to their records and cannot audit who has viewed which records. One of our stakeholders with both paper and electronic records limits access to protected health information as well as what the user can do with the data (view, modify, edit) based on the role of the individual. Audit trails track and monitor access to this information.

The third scenario initiated a discussion of whether or not a non-network provider would have access to the facility's records. Some of our stakeholders stated that the provider would need a contractual arrangement to access the facility's records while others stated that the access would be allowed with or without consent as provider to provider. Similarly, most of our stakeholders stated they would allow access to offshore transcription companies, if there was a contract in place with the company for transcription. None of them use off-shore transcription companies currently.

These business practices are all driven by policies within the organization that are created to protect patient privacy, within the parameters set by the technology used by the organization.

Information authorization and access controls present a barrier to health information exchange but it may be a necessary barrier to provide security and privacy to patient healthcare information. In addition, if access is limited and only certain components of a health record are viewable by certain employees within an organization, it will be difficult to exchange the protected information.

3 – Patient and provider identification

All of our stakeholders have policies to ensure when information is exchanged, that the correct patient information is exchanged. In these scenarios, patient verification is performed when information is requested and when patients are transferred between facilities. Most check the exact spelling of names and use two or three unique identifiers. Some use social security numbers and others just use middle initial and date of birth.

If a physician requests information from a facility, facilities often match varying combinations of the provider name, medical license number and provider signature.

When sensitive information is requested, the consent is used to verify the identify of the patient and the request form is used to verify the identify of the provider. Staff receiving the request

match components of the consent form to patient records to ensure that the appropriate patient's information is released. Some of our facilities match the signature of the consent with the patient's signature on file before releasing information. For organizations who also verify the provider, the medical license number and signature of the provider are used to verify the authenticity of the provider requesting the information.

Verification of the patient or provider is performed based on policies designed to protect the privacy of patient information. In general, practices are more stringent when sensitive information is being exchanged. Law does not govern the verification of the patient or provider.

Verification of the patient and provider are barriers to health information exchange. Without a master patient index, it is often difficult to find unique patient identifiers to ensure that the appropriate patient information is being exchanged. If information were exchanged on a national level, this issue would be exponentially amplified.

4 - Information transmission security or exchange protocols

The first transmission of information occurs when a request is made for patient information. The Variations Workgroup found variability in how requests for patient information are made. Some send written requests for patient information in the mail while others send via fax. If the physician has a relationship with the facility he is requesting from, or if it is a local physician, the physician typically calls a provider in the facility to make a request. These physician to physician requests over the phone are generally not documented.

If information is needed immediately, all workgroup members would fax the information, unless the requesting facility was in their network and had access to their medical record. If the information is not needed immediately, some would still fax, others would copy and mail. If the patient is being transferred from one facility to another, some facilities would send the paper chart with the patient while others would fax or mail the records.

Some organizations prefer to send medical records via US mail because they can copy the entire record and not remove elements that cannot be sent electronically. Others prefer to fax documents to reduce the cost of copying and mailing.

Although there are no legal requirements for mode of transmission, the variability in practice related to the request and disclosure may create barriers to health information exchange. Federal law does, however, control the security of transmission and the variability in implemented electronic systems and cost for secured transmission may present barriers to information exchange.

5 – Information protection (against improper modification)

Our stakeholders with electronic medical records have the ability to limit access to patient records to read-only, modify information or edit/delete information based on patient role. In addition, they have policies stating who can modify patient records. For the most part, organizations with paper records have policies that clearly state who can modify patient records. The small physician practice queried did not have policies stating who could modify records; instead they use "good practice" to determine who may edit patient records. Variability in

practice in relation to authorization for modification and protection of data integrity may create barriers in information exchange.

6 - Information audits that record and monitor activity

Each of the scenarios brought up areas where workgroup members record, monitor and audit the use of health information.

When information is released from one facility to another, our stakeholders varied as to whether or not they logged the release. Typically if medical records clerks release the information, they log the requestor name, facility/company, patient identification, date/time and purpose. For sensitive information, even though documentation of the release is required by law, some would document and others would not. For those who do document the disclosure, some releases are logged on paper, others in the patient's chart. If the organization uses an electronic medical record, often the technology itself would log the disclosure by capturing who accessed the information. While the practices stated above are the policies of the representative organizations, in practice all said that not every disclosure is documented, especially when the physicians disclose the information.

The organizations without electronic health records do not have systems for auditing or monitoring access to health information, while the facilities with electronic systems audit and monitor access. Typically, random reports are run by those with electronic systems to see who accesses which records. Many of our organizations always monitor access to VIP records.

The statutory requirements for documentation of disclosures, specifically under state law, were deemed onerous barriers to information exchange.

7 - Administrative or physical security safeguards

The third scenario initiated a discussion of physical security required for staff to enter facilities.

A clinician in a small practice did not require any identification to enter his building; however the other organizations in our workgroup required employees to wear some sort of identification badge. Some badges grant access to different parts of buildings and only during specified hours. These badges typically monitor who enters the building as well. Other badges are color coded to show to which department a staff member belongs.

The security of paper records is safeguarded by policies. Representative stakeholders stated that they have policies that records must remain in the building at all times. These policies are adhered to for the most part. Policies are stricter for records containing sensitive information.

Physical safeguards, as simple as requiring a key to enter a physician's office, although deemed necessary for privacy protection, result in barriers to information exchange.

8 – State law restrictions

The treatment scenarios highlighted many state law restrictions on the exchange of health information. In many cases, Wisconsin state law is more stringent than federal law, and this

creates a barrier to health information exchange. Barriers are also caused because in many cases, the law is not clear, and in practice interpretations of the law vary.

Consent

Wisconsin state law requires consent to release sensitive, more stringently protected, patient information, which includes mental illness, substance abuse or developmental disability. Wisconsin state law does not require a consent to release HIV test results from one provider to another for treatment purposes, however many of our stakeholders would require consent to release this information. Wisconsin state law (as well as federal law) requires consent to disclose patient information to a relative. If the patient is deceased, the legally authorized person must sign the consent.

Wisconsin state law requires several elements to the consent which vary from federal law. In general, most consent used in Wisconsin have both the Wisconsin and federal required elements.

Many of the requirements for obtaining patient consent and validating patient consent are considered onerous by the stakeholders.

Documentation of Disclosure

Wisconsin state law requires documentation of the release of sensitive information from provider to provider for treatment purposes. Law does not dictate how the documentation needs to be made and therefore there are wide discrepancies in documentation practices. Stakeholders regard the state documentation requirements as onerous.

Re-disclosure

There are Wisconsin requirements for disclosing health information obtained from another provider. However, there is variability among stakeholders in the application of the law. The re-disclosure provision creates difficulties in determining what information may be disclosed from a patient's record and therefore creates barriers to exchange.

9 – Information use and disclosure policy

Many of the business practices our stakeholders discussed for disclosure of information were governed by policies and many of the policies are in place to ensure compliance with State and Federal laws. The variation in practice and interpretation of law resulted in many business practices that may obstruct the exchange of health care information. A summary of the policies is below.

1. Obtain a declaration from the facility for the out-of-state facility that this is an emergency
 - The requestor must declare the purpose of request as a medical emergency. If request is verbal, requestor must state this is being declared a medical emergency and the clerk will document this in the request log. If request is via fax, email or paper, then it must be in writing that this is being declared a medical emergency.
2. Request information

- Nurse attempts to obtain consent from patient to request medical and mental health information. Consent is faxed along with request for information.
3. Verify requestor of patient information
 - All stakeholders have verification processes, but the policies vary.
 - Some verify requestor by requiring the request be made in writing on a recognizable letterhead
 - For phone requests, many ask for the phone number and call them back and others require a faxed request on letterhead.
 4. Obtain consent for release of information
 - Scenario 2: All stakeholders require a consent to release sensitive information
 - Scenario 3: Some of our stakeholders require consent for disclosure of sensitive information to the skilled nursing facility for ongoing treatment. Others do not require patient consent.
 - Scenario 4: Some stakeholders would require consent to release HIV test result information; others would not for treatment purposes. All stakeholders would require a consent signed by a legally authorized person to release information to the niece.
 5. Obtain consent to re-disclose information
 - There were variations in policies for re-disclosure of information. Some require a cover letter specifically giving authorization to re-disclose to accompany the patient consent.
 - Others treat the information as their own, and disclose per their disclosure policies.
 6. Limit information to be disclosed
 - All stakeholders have policies to limit the information disclosed to the minimum necessary for the purpose of the disclosure, even though it is not required for disclosure for treatment purposes.
 7. Integrate/accept patient information received from another source
 - Policies for integration varied:
 - One facility receives the information prior to patient arrival and integrates all relevant information into the patient chart. Remaining information is shredded.
 - One facility integrates the received information into the patient record, electronically when possible
 - One facility integrates the information into the patient chart
 8. Contract with off-shore transcription service to provide transcribed patient information
 - None of the facilities queried were allowed to contract with an off-shore transcription company
 9. A business associate agreement to protect the privacy of patient information
 - The physician transcription service is controlled by contract or business associate agreement

2.1.4 Critical Observations

Unique to Wisconsin

The treatment scenarios highlight 2 major barriers to health information exchange that are created by Wisconsin state law. The first is the requirement for a consent to exchange sensitive information for treatment purposes (mental health, alcohol or drug abuse, developmentally disabled) that is more stringent than federal law which does not require consent under these circumstances.

The second barrier, unique to Wisconsin, are the laws governing the documentation of disclosures of healthcare information. Legal requirements requiring documentation of disclosures make the exchange of healthcare information more difficult. Our stakeholders varied in their interpretation of the regulations, but each stated that documentation requirements pose a significant barrier to health information exchange.

Major Barriers to Exchange

Consent

Any time consent is required in order to exchange information, it creates a barrier to exchange. Differences in state and federal law regarding the required components of consent exacerbate the barrier. Most consents have both the state and federal requirements but when information is exchanged across state lines, the consent often does not meet the Wisconsin requirements and may therefore be considered invalid.

Consents are required by law in Wisconsin for the exchange of sensitive information unless the disclosure meets one of the very specifically defined and rigid exceptions. The Wisconsin law is also more stringent than the federal resulting in barriers to exchange across state lines. In addition, while not required by law, most stakeholders have policies requiring consents for disclosure of HIV test results, even for treatment purposes. The requirement of consent is driven by law and policy and poses barriers to information exchange.

Documentation of disclosures

State regulations requiring the documentation of disclosures pose significant barriers to exchange. The requirements are rigorous and difficult to interpret and therefore there are variations in how the documentation is completed. Our workgroup believes that technology may be able to automate the documentation process, significantly reducing and perhaps eliminating this barrier to exchange.

Verification of requester

Federal law mandates that the requester of health information be verified before health information is exchanged. Practices for verifying the requester vary and taking this additional step to verify the requester slows the exchange process.

Minimum necessary

Federal requirements to limit the exchange of health information to minimum necessary increase the amount of time required to exchange health information. Often technology cannot limit disclosures to the minimum necessary, so processes that could be electronic need to be manual so that the information can be manually limited. For organizations that use paper

records, sifting through records to make sure that the minimum necessary is exchanged is also time consuming, creating a barrier to exchange.

Re-disclosure requirements

State law has specific requirements for re-disclosure of health information. Not only is a barrier created by the requirements themselves, but varying interpretations of the law create inconsistent application and therefore a barrier to exchange.

Business associate agreements

The federally mandated requirement of an extensive and legally sound business agreement to allow exchange between a covered entity and a company using protected health information to do business may cause a barrier to information exchange.

Request for information practice

The variability in the process used for making the request for patient information - by phone, in writing, by fax, when linked with specific requirements for the format of requests creates barriers to efficient exchange of patient information.

2.2 Payment (Scenario 5)

2.2.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the payment scenario:

- Clinicians
- Consumers
- Federal Health Facilities
- Hospice
- Hospitals
- Long term care
- Payers
- Physician groups
- Physician groups

Please refer to section 1 for a detailed description of the stakeholders.

2.2.2 Summary of Findings

This section contains the scenario followed by the high level findings of the Variations and Legal Workgroups.

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

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

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

Variations Workgroup Summary

All relevant workgroup stakeholders agreed that they would not grant open access to the medical record to a payer because the technology cannot limit what the payer could see. Federal law requires that the provider limit access or disclosure for payment to the minimum necessary to achieve payment. Many stakeholders use paper-based charts that require allowing access to all patient information including information not relevant to payment or manually reviewing the record to determine what would be allowed to be accessible. Both processes are burdensome and time consuming for the provider. Others have electronic systems that cannot limit access to specific parts of the patient record and therefore cannot

meet the minimum necessary standard if payer access is allowed. The stakeholders uniformly agreed that payer access without the ability to limit access to specific payment information would be inappropriate and possibly a violation of patient privacy.

Legal Analysis

According to state and federal law, consent would not be necessary to release limited information related to the inpatient service that needed to be pre-authorized for payment purposes²¹. Federal law requires that the information disclosed for payment be limited to that which is minimally necessary to be able to make payment for the service provided.²² If the payer requested full access to the EHR, consent is required. If the payer requested information related to an HIV test result, mental health, alcohol, and drug abuse or developmentally disabled, consent would be required.²³

Verification of the provider would be required by federal law²⁴ and documentation of the disclosure for payment would be required by state law.²⁵

2.2.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 – Patient and provider identification
- 4 - Information transmission security or exchange protocols
- 5 – Information protection (against improper modification)
- 8 - State law restrictions
- 9 - Information use and disclosure policy

1 – User and entity authentication

For those represented organizations who would share their electronic health information with a payer, they would either require a written agreement or a business associate agreement between the health care provider and the payer. Many of our stakeholders would not grant access to a payer to any part of their health records.

In order to access the payer's system, users must login with a user name and password. Stakeholders agreed they would not allow access if their only access capability to the information would be unlimited access.

2 - Information authorization and access controls

²¹ Wis. Stat. 146.82(2)(a)3; 45 CFR §§164.502(a)(1)(ii) and 164.506(c)(3)

²² 45 CFR 164.502(b)(1)

²³ Wis. Stat. 252.15; Wis. Stat. 51.30; 45CFR 164.512

²⁴ 45 CFR 164.514(h)

²⁵ Wis. Stats. 146.82(2)(d); 51.30(4)(e)

In the one organization in our workgroup who allowed a payer access to their electronic medical record, the payer uses a login and password to access a specific portion of the record. This is currently only being done by a large hospital for a small HMO and a written business agreement exists between the two entities which states which parts of the record the payer can access.

Others with electronic medical records do not have the technology to limit access to a portion of a record or a subset of the patient population. Therefore granting access at all violates minimum necessary. A majority of our stakeholders have paper records and therefore this scenario does not apply to them.

The payers responding to the scenario stated that their systems provide role-based access, which is allowed by a password. If a user has access to the medical management file, they can access any patient record – the technology cannot limit access to a portion of the record.

3 – Patient and provider identification

Practices were not discussed because the participants would not exchange information in this way.

4 - Information transmission security or exchange protocols

In most cases, access was not granted because systems cannot control who/what information is disclosed. In the one case where access to the electronic record is provided, the payer had a login and password to access information directly in the system.

5 – Information protection (against improper modification)

In the one case where access to the electronic record is provided, the hospital granted read-only access to the payer when disclosure was allowed.

In the payer system users cannot change or delete any information that has been entered in the system. These policies are driven by regulations in administrative code.

8 – State law restrictions

Consent

Wisconsin state law does not require consent to access general health care information for payment purposes. However, state law does require consent to access sensitive (mental health, HIV, drug and alcohol and developmental disabled) information for payment purposes. For access to a complete health record, consent is required by state law.

Minimum Necessary

Federal and Wisconsin state law only allow access to the minimum necessary to achieve the purpose for the disclosure. However, with the exception of one hospital, current technology

does not allow limiting of access to the minimum necessary, so this law creates a barrier to exchange.

Documentation of Disclosure

Wisconsin state law requires documentation of disclosure for payment purposes. These requirements create barriers to exchange because the documentation process is time consuming and it varies from Federal regulations.

Confidentiality

Wisconsin state law requires the health plan to keep all information accessed confidential. This is a barrier to exchange because information obtained has to be handled carefully so that only people who need to access it can access the data.

9 - Information use and disclosure policy

The only policy discussed with this scenario is whether or not a health care provider would allow a payer access to their health records. In most cases, our stakeholders would not release this information outside a system network. The reason for this is technology limitations and the law – current technology cannot limit the information disclosed to the minimum necessary. If the payer was in their network, the information (both sensitive and non-sensitive) would be released.

2.2.4 Critical Observations

Unique to Wisconsin

The payment scenario highlights three barriers to health information exchange that are unique to Wisconsin. First, Wisconsin state law mandates verification of the requestor of sensitive health information. Verification practices vary and therefore create a barrier to health information exchange.

The second barrier, unique to Wisconsin, is the documentation of disclosure for payment purposes requirement. The law requires very specific documentation, which serves as a barrier to exchange. In practice, compliance with the law varies. The Variations Workgroup believes that with the appropriate technology, documentation of disclosures can happen automatically, eliminating the barrier.

The final barrier is the requirement for consent if the records contain sensitive information. Currently if a record contains sensitive information, most technology would not allow access to the portions of the record that did not contain sensitive information and therefore consent would be required to release information to a payer.

Major Barriers to Exchange

Technology

All of the stakeholders with electronic medical records (EMRs) who stated they would not allow access to a payer to their health records stated they would if their technology allowed them to limit access to only relevant parts of the record and only to specific records to comply with minimum necessary requirements. Furthermore, current technology cannot specify the type of access that is granted. There is no way to grant read-only vs. update access and no way to audit what information is retained by the payer.

Verification

State and Federal law require verification of the requestor. The process is time consuming and the law does not give guidance as to how to perform verification, so practices are variable.

Consent

State law requires consent to release the information to the payer if the record contains sensitive information. Because electronic medical records currently cannot limit access to sensitive information, this creates a significant barrier to exchange. Patient consent would be required before granting the payer access to the records.

Minimum Necessary

Because technology cannot currently limit access to records to a specific portion of the record, there is no way to exchange in this way without violating the minimum necessary requirements.

2.3 RHIO (Scenario 6)

Critical Observations

Wisconsin has a number of health information exchanges in the early stages of formation. Currently only the Wisconsin Health Information Exchange (WHIE) meets the definition of a Regional Health Information Organization (RHIO).²⁶ WHIE has established a formal governance and membership structure, but has not yet entered into the implementation stage or begun to exchange data.

Many of the issues that are addressed in this scenario have been considered in developing the governance structures for WHIE. For example, business associate agreements will allow for the greatest exchange of information, while still meeting the needs of the member organizations.

Additionally, in the process of developing information exchange, there has been intensive discussion about who “owns” the data and ensuring its validity. A statewide Action Plan, to be submitted to the Governor by the end of 2006, will serve as a catalyst for the development and implementation of RHIOs in Wisconsin. The issues related to ownership and use will continue to be addressed, and solutions will likely be found to allow for the sharing of health information for both treatment purposes and public health.

²⁶ RHIO: an independent corporation that is intended to operate an exchange of clinical health information among competing stakeholder organizations supporting multiple use cases (Gartner Health Care; U.S. Clinical IT Initiatives: A Hype Cycle; 13-16 November 2005; The Hyatt Regency Grand Cypress; Orlando, Florida)

2.4. Research (Scenario 7)

2.4.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the research scenario:

- Associations
- Clinicians
- Consumer
- Federal health facilities
- Homecare and hospice
- Hospitals
- Long term care facilities and nursing homes
- Medical and public health schools that undertake research
- Physician groups

Please refer to section 1 for a detailed description of the stakeholders.

2.4.2 Summary of Findings

This section contains the scenario followed by the high level findings of the Variations and Legal Workgroups.

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

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

Variations Workgroup Summary

The workgroup determined that actual practices are variable in determining whether patient consent or additional IRB approval would be required to allow exchange of information beyond the scope of an approved research project. Most would go back to the IRB for review for a 6 month extension. Some said that they would simply provide the data requested without IRB approval or additional patient consent. Others would require IRB approval and follow the IRB recommendations as to whether or not additional consent is required.

Legal Analysis

State and federal law require that certain legal requirements be met for patient information to be accessible for research purposes without patient consent. In this scenario, the Legal Workgroup made the assumption that the research project had been approved by the IRB and consent from the patient for the disclosure of information for research purposes would not be required. In this case, state requirements for release without consent²⁷ for research purposes are less stringent than HIPAA²⁸ and federal law would control. Therefore, consent would not be required for disclosures related to the IRB approved research project.

In this scenario, both requests for disclosure of patient information appear to be outside IRB approval and a patient consent would be required under both state and federal law to disclose for an additional six months of research or for a post-graduate paper. Another solution for disclosure might be to request guidance from the IRB relating to the disclosure requests.

2.4.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 - Patient and provider identification
- 4 - Information transmission security or exchange protocols
- 5 - Information protection (against improper modification)
- 9 - Information use and disclosure policy

1 - User and entity authentication

In all represented organizations, researchers would be required to give a login and password to access research data.

2 - Information authorization and access controls

In all represented organizations, research charts are maintained separately from the patient record such that only researchers have access to the research data.

3 – Patient and Provider Identification

Some of our representative organizations document patient participation in the patient chart. In order to document, office staff cross reference patients between the research charts and the patient records using patient identifiers (full name, middle initial and date of birth).

4 - Information transmission security or exchange protocols

²⁷ Wis. Stats. 146.81(2)(a)6, 51.30(4)(b)3, 252.15(5)(a)10

²⁸ 45 CFR 164.512(i)

Methods of how the researcher receives patient data vary across our representative organizations. Some receive patient data electronically while others receive it on paper. Another receives hand-written questionnaires from patients and transcribes them into an electronic chart.

5 – Information protection (against improper modification)

In all cases, the research chart is maintained separately from the patient chart. Patient information in the chart, therefore, is not modified through research.

9 - Information use and disclosure policy

Many of the business practices our stakeholders discussed relating to these research scenarios were governed by policies and many of the policies are in place to ensure compliance with state and federal laws. A summary of the policies is below:

1. Obtain consent to participate in the research study.
 - Most organizations require research consent, signed by parent or legal guardian and approved by the IRB for the research project.
 - Organizations varied as to who would obtain the consent (clinician, researcher).
 - The IRB determines whether or not to waive consent, but they have rarely, if ever, waived.
 - For true research projects, (not disease surveillance) a research consent would be obtained.
2. Researcher request to extend research 6 months
 - For most organizations, the IRB determines if the extension falls under the original consent. If it does not, an additional consent is obtained.
 - With at least one organization, in practice, the researcher would extend the research an additional 6 months without an additional consent, even with a written policy that all changes go to the IRB for approval.
3. Research request to use research data for white paper
 - All changes in protocol go to the IRB for approval. The IRB determines if the white paper falls under the original consent. If it does not, an additional consent is obtained.
 - With at least one organization, in practice, the researcher would receive access to the database without an additional consent, even with a written policy that all changes go to the IRB for approval.

2.4.4 Critical Observations

Unique to Wisconsin

There is nothing unique to Wisconsin state laws that impact this exchange.

Major Barriers to Exchange

Research Charts

Research charts are maintained separately from medical records and therefore data in research charts is difficult to exchange.

Consent

The law does not allow disclosure of research data outside the original research parameters without an additional consent. There are varying Interpretations as to whether or not consent is required for exchanging research data outside the original research parameters. This variation presents a barrier to exchange as well.

2.5 Law Enforcement (Scenario 8)

2.5.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the law enforcement scenario:

- Clinicians
- Consumer
- Hospitals
- Other (Large Clinics)
- Physician Groups

Please refer to section 1 for a detailed description of the stakeholders.

2.5.2 Summary of Findings

This section contains the scenario followed by the high level findings of the Variations and Legal Workgroups.

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

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

Variations Workgroup Summary

The workgroup assumed that the blood draw in this scenario was performed for treatment purposes.

All relevant workgroup stakeholders would require consent for disclosure to law enforcement or parents. The method of verifying the law enforcement request was variable (some required a written request, others verbal), as was the method of disclosure.

Legal Analysis

If the blood draw is performed for treatment purposes, consent is required for disclosure to law enforcement or to the parents as there is no statutory exception under Wisconsin law that allows for disclosure to either without patient consent.²⁹ If the blood draw had been performed at the request of law enforcement and not for treatment, the test result would not have been protected

²⁹ Wis. Stat. 146.82(1)

from access by law enforcement under Wisconsin law and the result would have been accessible to law enforcement.³⁰ Because the patient is of the age of majority in Wisconsin, consent would be required to release patient information to the parents.³¹

Federal law requires verification of the requestor³² and both state and federal law require documentation of the disclosures.³³

2.5.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 - Patient and provider identification
- 4 - Information transmission security or exchange protocols
- 6 - Information audits that record and monitor activity
- 8 - State law restrictions
- 9 - Information use and disclosure policy

1 – User and entity authentication

Each exchange in the scenario would require verification of the identity of the requestor of the information. However, compliance with the verification regulations is variable.

To verify the identity of law enforcement, some organizations ask law enforcement to put the request in writing on letterhead to verify the authenticity of the individual requesting the information and to make a formal request, while others see the law enforcement officer in uniform in the ER and do not ask for any additional identification.

Once consent is obtained to disclose to the parents, some organizations ask for identification from the parents while others provide the information to the individuals claiming to be parents.

2 – Information authorization and access controls

In order to disclose the requested lab results, the physician first accesses the lab results. The method of obtaining lab results is variable across our representative organizations. Some view lab results in a computer system, while others view a slip returned from the lab.

3 – Patient and provider identification

Prior to releasing information, the provider matches the identity of the patient to the request. Providers use varying combinations of unique identifiers to match the identity of the patient.

³⁰ Wis. Stat. 146.81(4)

³¹ Wis. Stats. 146.82(1), 146.81(5)

³² 45 CFR 514(h)(1)

³³ Wis. Stats. 146.82(2)(d), 51.30(4)(e); 45 CFR 164.528(a)(1)(i)

4 - Information transmission security or exchange protocols

Representative organizations vary in how they disclose information to law enforcement. Some verbally release only the specific information requested while others respond in writing (paper or fax). Most require consent to disclose, but others, if pressured by law enforcement, often disclose without consent.

To disclose the information to parents, most organizations verbally release the specific information requested if consent was obtained.

6 – Information audits that record and monitor the activity of health information systems.

While law mandates documentation of the release of information to law enforcement, in cases where the nurse or physician is pressured to release the information and does so without consent, there is likely not any documentation in the patient's file indicating the release of information. If the consent is obtained, the consent form signed by the patient serves as documentation of the release of the alcohol and drug test results to law enforcement.

If the physician disclosed the information verbally to the parents, even if consent is obtained, most agreed that the disclosure is rarely documented in practice.

8 – State law restrictions

Consent

Wisconsin state law requires consent to disclose drug and alcohol test results to law enforcement or to family members.

Documentation of Disclosure

Wisconsin state law requires documentation of disclosures to law enforcement and to the parent. In practice there are variations in whether or not disclosures are documented. If physicians or nurses are pressured by law enforcement to release information they may not document. If consent is signed, the consent serves as the documentation. Most would not document the verbal release of information to parents

Court Order

If consent is not obtained, Wisconsin state law requires law enforcement to obtain a court order to request the information.

Minimum Necessary

The information released is limited to minimum necessary to fulfill the request. This is controlled by HIPAA.

9 - Information use and disclosure policy

Several policies govern the exchanges of information in this scenario. The policies are mainly driven by state and federal laws.

1. Obtain consent for disclosure to law enforcement
 - The provider or other health care professional asks the patient to sign a release form for this information. The release contains specific language about what records are to be released.
2. Obtain consent for disclosure to parents
 - The provider or other health care professional asks the patient to sign a release form for this information. The release contains specific language about what records are to be released.
3. Limit the information to be disclosed
 - All limit the information released to what is requested – minimum necessary
4. Requirements for the request
 - Some have policies that a request from law enforcement for drug and alcohol test results has to be written on letterhead
 - Others required a faxed request on letterhead
 - In practice, some don't require a formal request if a uniformed law enforcement officer is in the ER

2.5.4 Critical Observations

Unique to Wisconsin

Wisconsin state law mandates documentation of disclosure of health information. Every disclosure must be documented and the state requirements for disclosure are more detailed than federal requirements. For release without consent, time, date, to whom, who released it and purpose of release are required to be documented.

Additionally, the requirement for consent is more restrictive than HIPAA for sensitive information.

Major Barriers to Exchange

Consent

Because we assumed this is a medical blood draw, most facilities would not release the information to law enforcement without consent. The process to obtain consent poses a barrier to exchange. Additionally, the consent must adhere to the statutory guidelines, which are different in Wisconsin than the federal guidelines. These discrepancies pose additional barriers to exchange.

Method of disclosure

The method of disclosure to law enforcement varies – it is most often verbal disclosure but some would print the result and give a copy of it to law enforcement.

Verification of the requester

Facilities vary in how they verify that the requester is legitimately law enforcement. They also had varying understandings of what is required from law enforcement to demand a blood draw without consent.

Documentation of the release

The law requires documentation of the release of information. However, compliance among stakeholders is variable. Both the requirements and the variances in interpretation of the requirements pose barriers to exchange.

Minimum necessary

The law requires the information released to be the minimum necessary to satisfy the purpose of the request. However, in order to limit the information prior to releasing it, staff must look through the record and filter the information. This is time consuming for paper records and impossible with current technology for electronic exchange.

2.6 Prescription Drug Use/Benefit (Scenarios 9 and 10)

2.6.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the prescription drug use/benefit scenarios:

- Clinicians
- Physician groups
- Federal health facilities
- Hospitals
- Payers
- Professional Associations
- Consumers or consumer organizations

Please refer to section 1 for a detailed description of the stakeholders.

Summary of Findings

This section contains each scenario followed by the high level findings of the Variations and Legal Workgroups.

Scenario 9 – Pharmacy Benefit Scenario A

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

Variations Workgroup Summary

The disclosure by the patient to the PBM is not protected because disclosure by a patient does not fall under the statutory privacy protection of patient information. However, the disclosure from the physician to the PBM is a protected disclosure and in practice, the relevant workgroup stakeholders agreed they would release the information to the PBM without a patient consent.

Stakeholders vary somewhat in whether they would involve the patient in this exchange rather than disclose directly to the PBM.

Legal Analysis

The Legal Workgroup agreed that a disclosure from the patient is not protected under state or federal law. Once the prescription is received, the PBM would be required to maintain the patient information in a confidential manner.

If the self insured hospital is considered to be a covered entity as either a hospital or health plan³⁴ under HIPAA, a business associate agreement would be required to enable the self insured hospital to share information with the PBM, a business associate providing services to the hospital.³⁵

If the Geodon prescription is considered general health information, a patient consent would not be required under state or federal law for an exchange between health care providers for treatment.³⁶

Documentation of the disclosure of general health information, although not required by federal law, would be required by state law and under the preemption analysis, state law would control.³⁷

If the Geodon prescription is considered to be mental health information, the controlling law would be Wis. Stat 51.30 and more stringent protections would apply. A patient consent for information exchange between the PBM and the prescribing physician would be required as there are no statutory exceptions for treatment or payment under this Wisconsin law.³⁸

Wisconsin Statute 51.30 would also require that the disclosure be documented, again preempting HIPAA which does not require this documentation under these circumstances.³⁹

State law is also more stringent than HIPAA in requiring the application of the minimum necessary standard to treatment information released for mental health information disclosures.⁴⁰ If the disclosure is for payment HIPAA would also require application of the minimum necessary standard.

If the exchange is electronic, HIPAA would require that the prescribing physician secure the transmission to the PBM.⁴¹

HIPAA would require the prescribing physician to verify the identity of the requestor, the PBM prior to allowing disclosure.⁴² There is no similar requirement in Wisconsin law unless the Geodon is mental health information and then verification of the requestor is also required under Wisconsin law.⁴³

Scenario 10 – Pharmacy Benefit Scenario B

³⁴ 45CFR 164.103

³⁵ 45 CFR 164.502(2)(e); 45 CFR 164.504(e); 45 CFR 164.506(c)(3)

³⁶ Wis. Stat. 146.82(2)(a)2; 45 CFR 164.506(c)2

³⁷ Wis. Stat. 146.82(d)

³⁸ Wis. Stat. 51.30(4)

³⁹ Wis. Stat. 51.30(4)(e)

⁴⁰ HFS 92.03(n)

⁴¹ 45 CFR 164 Subpart C

⁴² 45 CFR 164.514(h)

⁴³ HFS 92.03(1)(m)

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.

Variations Workgroup Summary

The workgroup agreed that a business agreement between Company A and the PBM's would be required to disclose information from one PBM to another. The information shared would be limited to the minimum necessary to accomplish the business purpose of the disclosure.

Legal Analysis

Company A, as a self insured business, would be considered a health plan under HIPAA and would be required to have a business associate agreement with both PBM1 and PBM2 to share protected health information. The business associates, through their relationship with the health plan, would be required to adhere to the restrictions of the HIPAA Privacy and Security Rules.⁴⁴

Unless Company A could be considered a health care provider under Wisconsin law, there would be no state privacy protection relating to this scenario. Exchange between these entities would be considered a "use", not a protected disclosure.

Under federal law, PBM2 would be required to verify the identity of the requestor PBM1.⁴⁵

If the sharing of information is electronic, under the HIPAA Security Rule, the exchange would be required to be secured.⁴⁶

Disclosures within this scenario would be controlled by the HIPAA minimum necessary standard.⁴⁷

2.6.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 - Patient and provider identification

⁴⁴ 45 CFR 164.504(e)(1)

⁴⁵ 45 CFR 164.514(h)

⁴⁶ 45 CFR 164 Subpart C

⁴⁷ 45 CFR 164.514(d)

- 4 - Information transmission security or exchange protocols
- 6 - Information audits that record and monitor activity
- 8 - State law restrictions
- 9 - Information use and disclosure policy

1 - User and entity authentication

Each of the two scenarios has a party requesting the information that should be verified.

For the PBM who is requesting information from the clinician, the clinician contacts the patient to determine whether or not the request is legitimate and if he could release the appropriate information.

For the second scenario, there would be an agreement between PBM 1 and PBM 2. This would most likely occur in a contract form. Relevant identifying information for both parties would be included in the contract.

2 - Information authorization and access controls

In the second scenario, the level of access given to PBM 2 would be stated in the contract and access to that information would be granted in accordance with the contract.

3 - Patient and provider identification

Prior to filling a prescription, the PBM checks patient's benefit levels and reviews prescriptions to ensure they are signed by a physician.

In order to authorize a prescription, nurses and physicians review the prescription and match the drug, physician and the patient to verify that the prescription is correct.

4 - Information transmission security or exchange protocols

In the first scenario, the prescription request was mailed by a patient directly to the PBM. The PBM then sends a request for authorization via phone or FAX to fill the prescription for a drug outside the health plan formulary. The physician usually gives the requested information back using the same means that the request was made.

Our workgroup determined that data sharing would not occur directly from the company to the pharmacy benefit manager with personal health information identifiers attached. Direct access into a PBM's data would typically not occur. Instead, access would be given by CD or other transportable device containing the minimum necessary data to meet the business requirements of the exchange.

6 - Information audits that record and monitor activity

In the first scenario, both the physician and the PBM would document the request for authorization by the physician. The physician documents the request for information directly in

the patient's record. The PBM uses a claims adjudication system which documents requests for information and requests for pre-authorization forms.

8 – State law restrictions

Consent

In Scenario 9, Wisconsin state law requires an informed consent from the patient in order for the physician to disclose information to the PBM. This is a requirement because Geodon is a mental health drug (51.30 – deemed part of the sensitive information statute). HIPAA would not require the consent.

De-identified Data

In Scenario 10, the workgroup assumed that the data was de-identified. De-identified data is not protected under the state or federal privacy laws and therefore, no consent would be required for exchange.

Self-insured Company

In Scenario 10, Company A is self-insured and therefore is not regulated as non-self-insured plans are. Wisconsin state regulations that govern exchanges between non-self-insured companies do not apply to Company A.

Business Agreement

In Scenario 10, Wisconsin state law does not regulate the exchange between the two PBMs because the exchange is a use, not a disclosure. However, HIPAA does require a business associate agreement, so following HIPAA, this exchange would require a business associate agreement.

9 - Information use and disclosure policy

Several policies govern the exchanges of information in these scenarios. The policies are mainly driven by state and federal laws.

Scenario 9

1. Document filling of patient's prescription
 - For drugs outside formulary for a given health plan, prior authorization from the physician is required. If the prescription is ultimately filled, then the pharmacist must retain a record of patient prescription outside of formulary.
2. Obtain consent to fill prescription
 - For prescriptions outside health plan drug formulary, the PBM sends an authorization form back to the patient, asking him/her to have his/her physician fill out a form to authorize the medication.

Scenario 10

1. Disclosure of patient information

- Sharing of data does not occur directly from the company to the PBM with personal health information identifiers attached.
- Access would be limited to the information required to perform the analysis
- 2. No consent required
 - Because the data is exchanged for payment purposes, there is no need for patient consent.
- 3. Business associate agreement required
 - Following federal law, the exchange of information between two entities for payment purposes requires a business associate agreement that includes mandated components. (164.504 (e) (1) 2, 164.501)

2.6.4 Critical Observations

Unique to Wisconsin

In Scenario 9, Wisconsin state law requires authorization for disclosure because the drug in question is a mental health drug. Therefore, the disclosure from the physician to the PBM requires a consent, which presents a barrier to exchange. Furthermore, the consent must meet the statutory requirements for a valid consent under Wisconsin state law, which serves as a barrier because the elements may differ from required elements in other states.

Wisconsin state law also requires documentation of disclosure (51.30 (4) (e)). HIPAA does not require documentation when the exchange is for treatment purposes. The discrepancy between Wisconsin and federal law as well as the documentation requirements both serve as barriers to exchange.

In Scenario 10, Wisconsin state law does not regulate this exchange because the exchange would be considered a use of information, not disclosure. However, HIPAA would require a business associate agreement for the exchange.

Major Barriers to Exchange

Consent

Consent is required for the physician to disclose information to the PBM for authorization for the drug. This is required by state law, not HIPAA. HIPAA allows treatment providers to share for treatment purposes without consent. The discrepancy between state and federal laws, the need for consent and the requirements of the consent all serve as barriers to exchange information.

Self-insured entities

Non regulation of self-insured companies may present barriers to exchange because they are not subject to state laws.

Business associate agreement

A business associate agreement is required for PBM 1 to share claims with PBM2. The creation of a business associate agreement that meets the needs of both the provider and the vendor can present a conflict in the protection of information. (federal law)

2.7 Healthcare Operations/Marketing (Scenarios 11 and 12)

2.7.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the Healthcare Operations/Marketing scenarios:

- Clinicians
- Federal health facilities
- Homecare and hospice organizations
- Hospitals
- Long term care facilities and nursing homes
- Physician groups

Please refer to section 1 for a detailed description of the stakeholders.

2.7.2 Summary of Findings

This section contains each scenario followed by the high level findings of the Variations and Legal Workgroups.

Scenario 11 - Healthcare Operations and Marketing - Scenario A

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

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

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

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

Variations Workgroup Summary

All relevant workgroup stakeholders stated that they would allow internal disclosure for quality assurance or service utilization purposes without patient consent. They would also allow internal disclosures of PHI to market targeted patient services without patient consent.

However, the stakeholders presented variable solutions to the internal exchange with marketing when the purpose of the disclosure was a mailing to a targeted patient population. Some stakeholders would require consent to disclose information to market educational services as some felt educational services were beyond treatment. The method for disclosure to an internal department was variable (paper report, electronic file), but all would limit the information provided to minimum necessary.

Legal Analysis

In this scenario the request for patient information is an internal request from one department to another either within a health care facility or within a healthcare network.

State law does not require verification of a requestor of identifiable patient information, however federal law does. That means that all covered entities must have written policies and procedures for verifying and authenticating the identity of a requestor of patient identifiable information.⁴⁸ Most responses from stakeholders indicated that knowing the requestor for an internal exchange would be sufficient verification of identity.

In Scenario 11, if ABC Healthcare is considered a network healthcare facility or an OCHA, both state and federal law would allow the internal sharing of identifiable patient information for quality assurance activities which fit under the definition of allowable health care operations. Both laws allow the sharing of information for health care operations without patient consent and the described activity with sigma six appears to meet the definition of health care activities.⁴⁹

Generally state law does not control an internal disclosure of patient information within a health care facility or network as it is considered an acceptable internal “use” where internal confidentiality policies, not state law, control the protection of the information. Generally, marketing activities are considered an internal “use” and would not be controlled by state law.

Federal law (HIPAA) has very specific guidance relating to the use of patient information for marketing activities. Since state law is silent unless a disclosure occurs, federal law, when applicable, controls internal use of patient information for marketing activities. HIPAA requires a patient consent for marketing activities.⁵⁰ The requirement of a patient consent for marketing activities does not apply if the activity does not meet the HIPAA definition of marketing.⁵¹ Based on the HIPAA exclusions from the marketing definition, the activity of the marketing department to send information to patients relating to the new rehab center and enhanced services available would not be deemed marketing as it is providing information to patients on hospital services.

State law does not control the internal transmission of patient identifiable data but federal law does. Federal law requires that security and privacy precautions be implemented regarding the internal transfer of patient identifiable data.⁵² This requirement, if deemed necessary, would be an impediment to the exchange of healthcare information.

⁴⁸ 45 CFR 164.514(h)(1)

⁴⁹ Wis. Stat. 146.82 (1); 45 CFR 164.501 Definitions; 45 CFR 164.506

⁵⁰ 45 CFR 164.508(a)(3)

⁵¹ 45 CFR 164.501 Definitions Marketing

⁵² Federal Security and Privacy Rules (HIPAA)

Federal law requires that the minimum necessary standard be applied to disclosures of identifiable information to an internal marketing department. Most of the stakeholders applied this standard when disclosing information to the marketing department.

Neither state nor federal laws require documentation of an internal disclosure for marketing.

Scenario 12 - Healthcare Operations and Marketing - Scenario B

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

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

1. To provide information on the hospitals' 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 use in marketing diaper services directly to parents.

Variations Workgroup Summary

All relevant workgroup stakeholders would disclose the patient information to marketing to provide information on a new pediatric wing. Some would disclose for marketing of educational classes. None would disclose for fundraising purposes or to sell the list to a diaper company. All varied in their mode of exchange (paper lists, files) and all would provide the minimum necessary – demographic information only.

Legal Analysis

In this scenario the request for patient information is an internal request from the marketing department to another internal department within a hospital facility.

State law does not require verification of a requestor of identifiable patient information however federal law does. That means that all covered entities must have written policies and procedures for verifying and authenticating the identity of a requestor of patient identifiable information.⁵³ Most responses from stakeholders indicated that knowing the requestor would be sufficient verification of identity.

Generally state law does not control a disclosure of patient information within a health care facility as it is considered an acceptable internal "use" where internal confidentiality policies, not state law, control the protection of the information. Generally, marketing activities would be considered an internal "use" and would not be controlled by state law. In the event that the

⁵³ 45 CFR 164.514(h)(1)

internal use results in an external disclosure, such as to a diaper company, then state law would treat that occurrence as a disclosure and state law privacy protections would apply.

Federal law (HIPAA) has very specific guidance relating to the use of patient information for marketing activities. Since state law is silent until a disclosure occurs, federal law, when applicable, will control internal use of patient information for marketing activities. HIPAA requires a patient consent for marketing activities.⁵⁴ HIPAA control over marketing is determined based on the HIPAA definition of marketing.⁵⁵

Based on the HIPAA exclusions from the marketing definition, the following communications under Scenario 12 would be excluded from HIPAA marketing control:

- To provide information on the new pediatric wing
- To provide information about parenting classes

Therefore the two activities that still require legal analysis are the exchange for fundraising and marketing with the diaper company. Since both the activities meet the HIPAA definition of marketing, a patient consent would be required for both of the activities under federal law. Since the exchange with the diaper company would be deemed a disclosure under Wisconsin law and there is not statutory exception for this type of disclosure, the exchange with the diaper company would also require a patient consent under Wisconsin law.

State law does not control the internal transmission of patient identifiable data but federal law does. Federal law requires that security and privacy precautions be implemented regarding the internal transfer of patient identifiable data.⁵⁶ This requirement, if deemed necessary, would be an impediment to the exchange of healthcare information.

Federal law requires that the minimum necessary standard be applied to disclosures of identifiable information to an internal marketing department. Most of the stakeholders applied this standard when disclosing information to the marketing department.

Neither state nor federal laws require documentation of an internal disclosure for marketing. However, if the use is deemed a disclosure, as in the relationship with the diaper company, documentation would be required under state and federal law.⁵⁷

2.7.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 - Patient and provider identification
- 4 - Information transmission security or exchange protocols
- 6 - Information audits that record and monitor activity
- 8 - State law restrictions
- 9 - Information use and disclosure policy

⁵⁴ 45 CFR 164.508(a)(3)

⁵⁵ 45 CFR 164.501 Definitions Marketing

⁵⁶ Federal Security and Privacy Rules (HIPAA)

⁵⁷ Wis. Stat. 146.82(d); 45 CFR 164.528

1 - User and entity authentication

The exchanges of information in these scenarios are internal. Verification processes for internal staff making request for non-sensitive patient identifiable records vary amongst our stakeholder organization. Some would simply verify the requestor by the fact that they know them personally. If the request is made electronically, the requester would be verified through the use of internal addressing options. Others require completion of a form for internal requests which contains required identifiers.

2 - Information authorization and access controls

For electronic internal requests for information, internal authorization and access controls are often used to limit the information that the requesting party has access to.

3 – Patient and provider identification

In order to process the request, all stakeholders had a process for ensuring the appropriate patients' information was disclosed to the internal department, however the methods for verifying that the appropriate patients' information is released vary widely. Methods include:

- Specific patient identifiers such as time frames and diagnosis codes
- Standard questions to elicit specific information to identify patient population
- State specific patient identifiers on the written request form
- Unique master patient identification number and specific diagnosis codes available within the information systems.
- Patient-specific, quality-controlled indicators such as specific diagnosis codes to sort for the requested information

4 - Information transmission security or exchange protocols

Our representative organizations reported varying methods for making internal requests for disclosure of health information. Some make requests between departments by phone, internal e-mail or internal mail. Others require a written request with a standardized form sent to medical records.

Likewise, there are varying methods of disclosure of information between departments.

Methods of transmission include:

- Send a paper copy of the information requested
- Send an email attachment with the requested information
- Send paper or email, depending on the request
- Create a database for the internal department, store it on a network drive and grant access to the requesting department.

In all cases, transmission of data is limited to the minimum necessary. For marketing purposes, the only information provided would be demographic data for mailings.

6 - Information audits that record and monitor activity

Document internal disclosure of information for marketing. In all cases, the disclosure would not be documented separately, but the disclosure itself would serve as documentation of the disclosure. If done electronically, systems would generate reports to document the exchange. When a form is used, the form serves as documentation.

8 – State law restrictions

Wisconsin state law does not regulate internal disclosures of health information. This scenario would be governed by Federal laws. This exchange would be governed by federal laws including:

The Federal Privacy Rule

Federal law does not require consent for a disclosure for quality assurance as it is deemed healthcare operations. However, federal law requires patient consent for a disclosure for marketing. In the above scenarios, marketing of patient products and patient treatment enhancements such as the rehab facility, the newborn wing and the parenting classes would not be considered marketing and would not require a patient consent. Fundraising and the disclosure to the diaper company would be HIPAA controlled marketing activities and would require patient consent for this type of activity.

Minimum Necessary

Federal law requires that the minimum necessary standard be applied to internal uses such as quality assurance and marketing.

9 - Information use and disclosure policy

Several policies govern the exchanges of information in these scenarios. The policies are mainly driven by state and federal laws.

1. Method used for making internal request for disclosure
 - One facility requires the request to be made in person to an administrator who would determine if the request was appropriate
 - One facility requires requests to go directly via paper, email or phone, to the medical records department for processing
 - One facility requires a form to be completed and sent to medical records for processing
 - One facility requires the request to be sent to the Privacy Officer who makes a determination of whether the information use is appropriate
2. Disclose information to internal marketing team
 - To market a new facility:
 - One facility does not send marketing materials directly to patients. Instead, materials are sent to providers who make appropriate materials available to patients

- One facility does not provide health information to internal departments for marketing purposes
- Internal exchange for marketing health care services is allowed in several organizations without patient consent
- One requires Board approval for using patient data to generate a mass mailing list for marketing purposes
- One organization puts a condition on similar requests that the privacy officer must see the information before it is distributed.

To request donations:

- Some facilities release demographics to request donations
- Others do not release demographics to request donations

To sell data to a third party:

None of our stakeholders release demographics for marketing purposes such as to a third party diapering service.

For quality assurance:

- All facilities queried provide identifying patient information between departments upon request for quality analysis of patient services

3. Method of disclosure

- One facility provides a paper copy of the information requested
- One facility provides the data electronically by e-mail
- Some facilities use both electronic and paper exchanges for internal requests depending on electronic capabilities for exchange
- Some facilities would use a shared drive folder for exchange

4. Specific information disclosed upon receipt of internal departmental request for identifying patient information

- All our stakeholders limit the amount of information disclosed to the minimum necessary to meet the needs of the requester

2.7.4 Critical Observations

Unique to Wisconsin

Wisconsin state law does not regulate internal disclosures of health information. Therefore, the exchanges that do not result in disclosures in the scenario do not present barriers to health information exchange that are unique to Wisconsin. The disclosures that would be considered internal marketing would be for the newborn wing, parenting classes and fundraising. However, if the internal marketing activity results in what could be deemed a disclosure of patient identifiable information such as the sale of information to the diaper company, Wisconsin law would regulate the disclosure. Since it does not fall under a statutory exception, a patient consent would be required for the disclosure to the diaper company. The requirement for a consent is consistent with federal law as well.

Major Barriers to Exchange

Method of requesting information

There were significant variations in the methods used for making the internal request for patient information, by phone and in writing. This variability when linked with specific requirements for verification of the requestor results in barriers to efficient exchange of patient information.

Method of exchange

The exchange of information is typically done via paper or in separate electronic files stored on a network server. The inconsistency in exchange and variability in processes for disclosure present a barrier to health information exchange.

Minimum necessary

Several stakeholders applied the minimum necessary standard when disclosing patient information for marketing and several did not. This variability in the application of the minimum necessary standard may present a barrier to information exchange.

Consent

Variable interpretation of legal requirements for consents resulted in policy requirements being implemented that were more stringent than the law. Some organizations have policies that do not allow the internal exchange of information without patient consent. Because it does not make sense to obtain patient consent to send the patient marketing materials, the policy requiring patient consent effectively stops all internal exchange of information in these cases and presents a major barrier to health information exchange.

2.8. Public Health/Bioterrorism (Scenario 13)

2.8.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the bioterrorism:

- Clinicians
- Physician groups
- Federal health facilities
- Hospitals
- Laboratory
- Public Health Agencies
- State Agencies
- Professional Associations
- Consumers or consumer organizations

Please refer to section 1 for a detailed description of the stakeholders.

2.8.2 Summary of Findings

This section contains the scenario followed by the high level findings of the Variations and Legal Workgroups.

Scenario 13 – Bioterrorism event

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

Variations Workgroup Summary

All the exchanges fit under statutory authority that allow release of patient information without a consent. The Governor has the power to issue a state of emergency to allow all of these exchanges under state law without consent. The responding stakeholders agreed that this scenario would allow for exchange without patient consent.

Anthrax is not only a bioterrorism agent, but it also occurs naturally in the environment and is transmitted through animals. Upon suspicion of an anthrax exposure, the physician is responsible for reporting to the local public health department. This report triggers an investigation into the cause: natural or manmade. If it is suspected that it is a bioterrorism event, a coordinated investigation with local, state and federal representatives begins, in order to establish the degree of threat to the public.

Identified information could be released without consent to all of the following as part of the ongoing investigation, once bioterrorism was suspected:

- Local public health department
- State public health department
- Centers for Disease Control and Prevention (CDC)
- Federal Bureau of Investigation (FBI)
- Homeland Security (no obligation to provide identifiable information)

Transmission of health information would commonly occur by fax and phone, until a bioterrorism event was declared, which triggers the incidence response process (IRP). The incidence response process would override all business practices if this was determined to be a positive anthrax event and categorized as a bioterrorism event. The IRP would rule the actions taken and the means by which information is disclosed and to whom. Determinations about the level of information provided are on a case-by-case basis.

Legal Analysis

State and federal law either mandates or allows disclosure of a positive lab test for anthrax without a patient consent to the patient's treating provider, local public health, state agencies with a statutory need to know and federal agencies that provide emergency public health services.⁵⁸ Anthrax is a category 1 communicable disease which means notification must occur within 24 hours to the local health officer.⁵⁹ According to Wis. Stat. § 252.03(2), local health officers may do what is reasonable and necessary for the prevention and suppression of disease and according to Wis. Stat. § 252.02(1), the department may also establish systems of disease surveillance and inspection to ascertain the presence of any communicable disease.

The Wisconsin Department of Health and Family Services (DHFS) is provided with broad authority and emergency management powers under Wisconsin Statute, § 252; where the department may authorize and implement all emergency measures to control communicable diseases, including anthrax. According to Wis. Stat. § 252.02(6), the department may authorize and implement all emergency measures necessary to control communicable diseases. This statute also requires physicians, health care facilities and laboratories that know or have reason to believe that a person treated or visited by him/her has a communicable disease shall immediately report to their local health officer. The local health officer shall report this information to DHFS.⁶⁰ These powers defined in this statute allow the removal of barriers to allow rapid and effective responses to an anthrax threat. Local health officers are provided with similar powers as the Department, however, need to keep the Department updated of measures

⁵⁸ HFS 145.04(2) (d)

⁵⁹ HFS 145.04(2)(d)

⁶⁰ HFS 145.04(2)(d)

taken. In addition, Wisconsin is part of an informal grouping of states (Greater Board of Health Initiative) which will share data interstate, in the event of communicable diseases.

State law allows the Governor to declare an emergency and that order empowers the exchange of information relating to a communicable disease.⁶¹

Wisconsin also has an electronic health network that provides primary information and timely communications about public health threats. This information is distributed in a number of forms, including fax blast, e-mail, by mail, etc. to all providers, public health agencies, to help them understand the threat and be alerted to possible cases. This communication most likely will not identify patients by name, however may have other elements of protected health information such as demographic, age, gender, etc. However, if identifying the patient is necessary to help find cases of anthrax, then identities may be disclosed as permitted by Wisconsin law. In cases where the law does not explicitly allow the disclosure, there would be no security or privacy barriers in exchanging this information; the balancing of privacy versus protecting public health would be weighed.⁶²

The Federal Privacy Law (HIPAA) also provides for the disclosure of patient information without patient consent under this scenario through the exceptions allowing for disclosure when required by law, for public health purposes and for public oversight.⁶³

State and federal law also require the documentation of disclosures within this scenario, although the stakeholder practices were variable.

2.8.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 - Patient and provider identification
- 4 - Information transmission security or exchange protocols
- 5 - Information protection (against improper modification)
- 6 - Information audits that record and monitor activity
- 7 - Administrative or physical security safeguards
- 8 - State law restrictions
- 9 - Information use and disclosure policy

1 – User and entity authentication

This exchange had numerous requests and exchanges relating to patient information. The first exchange was from a lab with a positive anthrax test to a local public health department. This is within the mandated reporting requirements of state law. In this case the lab report would have been sent without a request. Then exchanges occurred between county public health departments and then the state. None of these exchanges involve requests. Verification between the local and state public health agencies is done through verbal communication within

⁶¹ Wisconsin law Chapter 153

⁶² Wis. Stat. 252.02(6)

⁶³ 45 CFR 164. 512 (a) and (b)

the community of public health professionals. No direct verification of the individual would be necessary.

Requests for information may have come from state teams or the media and since the state has the authority to make the disclosure, verification of the requestor, although required by federal law, was not discussed.

2 – Information authorization and access

Access controls to patient information were also uniformly utilized. Access is controlled at the local public health agency by providing designated contact information for reporting these conditions to providers and labs. Established policies and process are invoked when health information about a reportable condition is supplied. These policies and procedures are role-based within the local public health agencies.

In addition, all stakeholders queried employed some type of physical identification within their organization - a method commonly used to identify employees for the purpose of physical access to a building and then ultimately to patient information. Often the badges used contain authorization for accessing certain physical locations within the building. Restricted access can be in the form of limited hours or areas such as medical records.

3 - Patient and provider identification

The representative organizations each used verification procedures for cross-matching identities to verify the providers of services such as the lab. The public health agency would receive the report from the lab through a fax on the lab letterhead, most often with a follow-up phone call, for any mandatory reportable condition. The local public health agency would verify the identity of the lab based on some identifying information received through the call or on the results submitted, such as a lab ID number. This would allow the public health agency to verify that the provider was in fact a specific lab.

The stakeholders also used methods to verify the identity of the patient. The infection control staff would verify the patient identity using two patient identifiers before releasing any information or taking any action related to a reportable condition. Information about the incident is submitted on a standard form provided by the local public health agency. This form includes information about the subject as provided by the clinician.

4 - Information transmission security or exchange protocols

The stakeholders used a variety of exchange methods. The Federal Security Rule would control the requirements for any electronic exchanges since state law does not provide transmission requirements. The Security Rule requires that the transmission meet federal requirements for a secure transfer of information. The lab would disclose the reportable condition to the patient safety office (within a hospital or clinic) through a direct phone call or through the infection control staff. The local public health agency would provide a copy of the case investigation form by fax and would receive the report through a fax on the lab letterhead, most often with a follow up phone call, for any mandatory reportable condition. The state public health agency would receive information either by fax or verbally and would release information to law enforcement,

hospitals, hazmat teams, or regional media, verbally or through a press release, limiting the information released to information necessary to protect the public health. An alternate mode of transmission is blast fax to all hospitals and hazmat teams.

Information regarding the reportable condition would be provided to hospitals and clinics via a secure electronic portal. This information would include basic demographic information, but not identified information. This release of information would be done through one of three mechanisms, depending on the level of threat to the public. Electronic exchanges such as this would be controlled by the Federal Security Rule. Release of information among the infection control staff within the hospital occurs through verbal messages.

The variable and somewhat unsecured methods for information exchange appear to exemplify variable compliance with federal law. Although the somewhat free exchange of information in this scenario implies little barrier to information exchange, in fact, the variability of interpretation, application and implementation of exchange methods result in barriers to health information exchange.

5 - Information transmission (against improper modification)

The workgroup did not specifically address electronic methods for assuring the integrity of information during exchange such as encryption or secured portals. However, there was a feeling among the responders that use of fax and verbal communication was a secure method of exchange that assured protection of the integrity of the patient information.

6 - Information audits that record and monitor activity

Generally, any methods that document disclosures were viewed to be an audit tool for evaluating where information has been sent. The public health agency retained copies of required forms to validate that information had been sent and to whom. Other documentation included actual documentation of the positive lab results by the lab, local public health or the state agency. The local public health agency would document the release of information, most likely in the case investigation file, possibly on the case investigation form. The lab would document in the case file the release of the positive lab result to the state lab, the physician, and the local public health department and infection control.

7 - Administrative or physical security safeguards

The stakeholders uniformly used physical security measures within their facilities relating to personnel access. All stakeholders listed some form of physical identification within their organizations. Often the badges used contained authorization for access to physical locations within a building.

8 - State law restrictions

Consent

Both state and federal law allow the exchange(s) of information in this scenario without patient consent. The stakeholders allowed exchange without patient consent and cited policy and law

as the drivers. The lab reported that they would report the positive lab results without consent to the state lab, physician, local public health department and infection control. The local public health agency would provide a copy of the case investigation form by fax, without consent, to the state agency.

Documentation of disclosure

State law would require documentation of a disclosure to a state lab.

Mandated reporting

State law mandates reporting of the anthrax lab results and compliance with this statutory requirement did not seem problematic to providers. The lab is required to report information about a positive anthrax result. Clinicians are required to report a suspected incidence of anthrax.

State and federal law also provide wide-based authority for the exchange of a positive anthrax test as a means to protect public health.

Federal law also requires verification of the requestor, secured transmission of the information and application of the minimum necessary standard when the information disclosed does not relate to treatment. There was variable compliance with these requirements.

9 - Information use and disclosure policy

Several policies govern the exchanges of information in these scenarios. The policies are mainly driven by state and federal laws.

1. Obtain consent for disclosure of patient information
 - The local public health agency would provide a copy of the case investigation form by fax without consent to the state agency.
 - The lab would report the positive lab results without consent to the local public health department through a fax on letterhead, most often with a follow up phone call, for any mandatory reportable condition.
 - The lab would report the positive lab results without consent to infection control staff within the hospital through a telephone call for a reportable condition.

2. Determine which information to disclose
 - The local public health agency would provide a copy of the case investigation form by fax without consent to the state agency.
 - The patient safety office or infection control would document the reportable condition, which would then initiate an incidence response.
 - The public health agency would release only as much information as necessary to the local public health department in another state to complete its investigation.
 - The public health agency would release only as much information as necessary for people affected by the reportable condition to complete its investigation.

3. Method for exchange of patient information (electronic or paper)
 - The local public health agency would receive the report through a fax on the lab letterhead, most often with a follow up phone call, for any mandatory reportable condition.
4. Documentation of disclosure of patient information
 - The patient safety office or infection control would document the reportable condition, which would then initiate an incidence response.
 - The local public health agency would document the lab results, most likely through the creation of their own case record. This would be supplemented with case investigation material.

2.8.4 Critical Observations

Unique to Wisconsin

One requirement unique to Wisconsin in this scenario is the requirement of providers to document disclosures.

The state authority to disclose patient information under this scenario is similar to disclosure allowed under federal law. The observed differences would probably be in state laws and differences would create barriers to exchange.

Major Barriers to Exchange

No overt barriers observed. Wisconsin's information sharing environment allows for easy sharing of information for bioterrorism events. Typically, the minimum amount of information necessary is provided, but whenever the public's health is at stake, personal health information may be provided.

Documentation of disclosure

Wisconsin state law would require the documentation of the disclosure to a state lab. State regulations requiring the documentation of disclosures pose significant barriers to exchange. The requirements are rigorous and difficult to interpret and therefore there are variations in how the documentation is completed. This workgroup believes that technology may be able to automate the documentation process, significantly reducing and perhaps eliminating this barrier to exchange.

Verification of requester

Federal law mandates that the requester of health information be verified before health information is exchanged. Practices for verifying the requester vary and taking this additional step to verify the requester slows the exchange process.

Minimum necessary

Federal requirements to limit the exchange of health information to minimum necessary increase the amount of time required to exchange health information. Often technology cannot limit disclosures to the minimum necessary, so processes that could be electronic, need to be manual so that the information can be manually limited. For organizations that use paper records, sifting through records to make sure that the minimum necessary is exchanged is also time consuming, creating a barrier to exchange.

Re-disclosure requirements

State law has specific requirements for re-disclosure of health information. Not only is a barrier created by the requirements themselves, but varying interpretations of the law create inconsistent application and therefore a barrier to exchange.

Request for information practice

The variability in the process used for making the request for patient information - by phone, in writing, by fax, when linked with specific requirements for the format of requests creates barriers to efficient exchange of patient information.

2.9. Employee Health (Scenario 14)

2.9.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the employee health scenario:

- Clinicians
- Consumers
- Federal Health Facilities
- Hospitals
- Payers
- Physician groups
- Professional Associations

Please refer to section 1 for a detailed description of the stakeholders.

2.9.2 Summary of Findings

This section contains the scenario followed by the high level findings of the Variations and Legal Workgroups.

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

Variations Workgroup Summary

It was the general consensus of the stakeholder group that they would not release without a patient consent under the facts presented in this scenario. In practice, some of our workgroup members would require a consent to disclose the information to the employer while others would disclose directly to the patient and not require a consent. None of the workgroup members would disclose the information electronically – it would all be done via paper form, either mailed or faxed. All would disclose the minimal information necessary to complete the request.

Legal Analysis

State law does not require verification of a requestor of identifiable patient information, however federal law does. Therefore all covered entities must have written policies and procedures for verifying and authenticating the identity of a requestor of patient identifiable information.⁶⁴

⁶⁴ 45 CFR 164.514(h)(1)

State and federal law require a patient consent to disclose the patient's medical information related to the back-to-work form from the provider to the employer.⁶⁵

Wisconsin law and the federal privacy law do not require a consent for release of information to the patient. Therefore, if the form validating the employee's return to work is provided to the patient, no consent is required.⁶⁶ A provider, under the Federal Privacy Rule, may require that the request for information from the patient be provided in writing.

The Federal Privacy Rule requires that the provider releasing the patient back-to-work information apply the HIPAA minimally necessary standard in relation to the information released.⁶⁷

Both state and federal law requires documentation of a disclosure to the patient's employer.⁶⁸

Only state law requires documentation of disclosure to the patient.⁶⁹

2.9.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 4 - Information transmission security or exchange protocols
- 6 - Information audits that record and monitor activity
- 8 - State law restrictions
- 9 - Information use and disclosure policy

4 - Information transmission security or exchange protocols

This scenario has two exchanges of information. First, the provider receives a request for return to work form from the employer, then the physician completes the form and returns it to the provider.

The first exchange typically occurs with a paper form mailed from the employer to the provider. Occasionally, a facility will receive an email request from a patient to complete a return to work form.

In the second exchange, the physician writes a prescription indicating that the patient can return to work and sends it to the employer. In some cases, the return to work form is a standard piece of the discharge materials provided to the patient. When provided directly to the patient, the patient is responsible for giving the form to the employer.

6 - Information audits that record and monitor activity

⁶⁵ Wis. Stats. 146.82(1), 51.30(4)(a), 252.15(5); 45 CFR 164.508

⁶⁶ Wis. Stats. 146.83, , 252.15(5)(a); IHFS 92.05; 45 CFR 164.524

⁶⁷ 45 CFR 164.514(d)

⁶⁸ Wis. Stats. 146.82(d), 51.30(4)(e); 45 CFR 164.528

⁶⁹ Wis. Stats. 146.83, 51.30(4)(e)

Business practices vary as to the extent of documentation of the release of return to work to the patient or the employer. The physician may or may not document the release in the patient's chart. In some facilities, the form is always copied and placed in the patient chart before it is given to the patient. In others, if the form is provided directly to the physician, the release is rarely documented in the record.

8 – State law restrictions

Consent

Wisconsin state law and federal law require a patient consent to release identifying patient information to the patient's employer. The form from the employer typically includes a standard release statement. The consent must meet the statutory requirements and state and federal requirements vary. A consent is not required for release of information directly to the patient.

Documentation of Disclosure

Wisconsin state law and federal law require documentation of the disclosure to the employer. While required by law, compliance is variable. If the form is provided directly to the physician, it is rarely documented.

Wisconsin state law requires documentation of disclosure made directly to the patient. Compliance with this is variable. Some copy the work slip and place it in the patient record. With others, if the form is provided to the physician, it is rarely documented. However, the documentation regulation presents a barrier to exchange.

9 - Information use and disclosure policy

Several policies govern the exchanges of information in these scenarios. The policies are mainly driven by state and federal laws.

1. Process request from an employer to validate a patient's return to work
 - For some, a return-to-work form is standard within the discharge materials provided in the ER.
 - For others, there is no policy governing this exchange. The provider would provide the information requested, limiting it to minimum necessary.
2. Release with consent of return to work form from facility to employer
 - The facility receives forms from employers, which typically include a standard release statement.
3. Physician/provider release the minimum necessary to meet the request for information
 - The clinician would provide the minimum information necessary on a standard form provided by the facility indicating that the patient was able to return to work.
 - The information provided would not include any information about the diagnosis
4. Documentation of disclosure to patient

- All facilities have policies mandating the documentation of the disclosures to the patient or the employer, but compliance with the policies is variable

2.9.4 Critical Observations

Unique to Wisconsin

The only requirement unique to Wisconsin in this scenario is the requirement of the provider to document the disclosure to the patient. Compliance with this law is variable, but the regulations pose a barrier to exchange because the requirements are time consuming.

Major Barriers to Exchange

Consent

Wisconsin state and federal law require patient consent to disclose the information to the employer. State and federal requirements of the consent vary and therefore most consents produced in Wisconsin satisfy both requirements. Both the obtaining consent and the requirements of the consent specific to Wisconsin serve as barriers to exchange.

Documentation of disclosure

Wisconsin state law requires documentation of the disclosure of information to the employer or the patient. While compliance with the regulations varies, the requirements to document the release of information pose a barrier to exchange.

Comments

This exchange rarely occurs between an employer and a physician – the exchange is typically between the physician and the patient and then the patient and the employer.

2.10. Public Health (Scenarios 15–17)

2.10.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the employee health scenario:

- Clinicians
- Consumers
- Correctional facilities
- Federal health facilities
- Hospitals
- Laboratories
- Other (Large clinics)
- Other (Small clinics)
- Payers
- Public Health
- State Government

Please refer to section 1 for a detailed description of the stakeholders.

2.10.2 Summary of Findings

This section contains the scenario followed by the high level findings of the Variations and Legal Workgroups.

Scenario 15 – Public Health - Scenario A - Active carrier, communicable disease notification

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

Variations Workgroup Summary

Under Wisconsin state law, State A would disclose personal health information to State B in this scenario. The state would contact the local public health department who would provide further disclosure. If the bus is in Wisconsin, or law enforcement contact is needed in Wisconsin, the state has the authority to make the contact without patient consent.

No barriers to exchange were discussed for the public health scenarios. Wisconsin's information sharing environment allows for the sharing of information for mandatory reporting for public health purposes, such as communicable diseases.

Typically, the minimum amount of information necessary is provided, but whenever the public's health is at stake, personal health information may be provided.

Public health staff have the ability to share the information necessary to protect the public. In practice, staff provide only the minimum information necessary to conduct the necessary investigation or to determine the level of exposure for the patient's fellow passengers.

When consent is deemed necessary, the process can be cumbersome, but is not necessarily a barrier to the exchange of information.

Legal Analysis

State and federal law either mandates or allows disclosure of communicable diseases such as TB without a patient consent to the patient's treating provider, local public health, state agencies with a statutory need to know and federal agencies that provide emergency public health services.⁷⁰ According to Wis. Stat. § 252.03(2), local health officers may do what is reasonable and necessary for the prevention and suppression of disease and according to Wis. Stat. § 252.02(1), the department may also establish systems of disease surveillance and inspection to ascertain the presence of any communicable disease.

The Wisconsin Department of Health and Family Services (DHFS) is provided with broad authority and emergency management powers under Wisconsin Statute, § 252, where the department may authorize and implement all emergency measures to control communicable diseases, including TB. According to Wis. Stat. § 252.02(6), the department may authorize and implement all emergency measures necessary to control communicable diseases. This statute also requires physicians, health care facilities, and laboratories that know or have reason to believe that a person treated or visited by him/her has a communicable disease, and shall immediately report to their local health officer. The local health officer shall report this information to DHFS.⁷¹ These powers defined in this statute allow the removal of barriers to allow rapid and effective responses to a TB threat. Local health officers are provided with similar powers as DHFS, however, must keep DHFS informed of measures taken. In addition, Wisconsin is part of an informal grouping of states (Greater Board of Health Initiative) which shares data interstate, in the event of communicable diseases.

Wisconsin also has a health network that provides primary information and timely communications about public health threats. This information is distributed in a number of forms, including fax blast, e-mail, by mail, etc. to all providers and public health agencies to help them understand the threat and be alerted to possible cases. This communication most likely will not identify patients by name, however may have other elements of protected health information such as demographic, age, gender, etc. However, if identifying the patient is necessary to help find cases of TB, then their identities may be disclosed as permitted by Wisconsin law. In cases where the law does not explicitly allow the disclosure, the balancing test of privacy versus protecting the public would be weighed. There are no security or privacy barriers in exchanging this information.⁷²

⁷⁰ HFS 145.04(2) (d)

⁷¹ HFS 145.04(2)(d)

⁷² Wis. Stat. 252.02(6)

The Federal Privacy Law (HIPAA) also provides for the disclosure of patient information without patient consent under this scenario through the exceptions that allow for disclosure when required by law, for public health purposes and for public oversight.⁷³

State and federal law also require the documentation of disclosures within this scenario, although the stakeholder practices were variable.

Scenario 16 – Public Health – Scenario B – Newborn screening

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

Variations Workgroup Summary

In this scenario, the Variations Workgroup determined that the exchanges of health information would occur differently than stated in the scenario.

The positive test result for a state-mandated screening test triggers a series of events, including reporting to the state public health department, physician, and the state registry. The state has the authority to conduct the test and contact both the physician and the patient (or family) without consent. In Wisconsin, the state lab only contacts the provider or the patient's family – they do not contact the specialty care centers. The state lab maintains a registry, which is mandated by Wisconsin state law, however the registry does have an opt out provision - parents of children with positive screening results may sign a form and opt out of the state registry. Currently, this exchange of information occurs through a secure web-based portal. The only piece that is not automated is the transfer of the newborn information and test material to the state lab. The state can also disclose to public health departments without patient consent.

Legal Analysis

Disclosure of patient information

The Legal Workgroup analyzed the following exchanges of health information related to this scenario:

1. Hospital to state lab

Wisconsin law requires screening for congenital disorders of all newborns, which are to be submitted and processed through the state lab (Wisconsin Statutes 253.13). This scenario presents a similar process to that authorized by Wisconsin law.

2. State lab to the physician

⁷³ 45 CFR 164. 512 (a) and (b)

Wisconsin law mandates disclosure of the screening lab result from the state lab to the physician [Wisconsin Statutes 253.13(4)], and the HIPAA Privacy Rule allows for disclosures without patient authorization when a use/disclosure is required by law or for public health activities [45 CFR 164.512(a) and (b)]. In Wisconsin the physician is also mandated to provide the results to the parents or legal guardian.

3. State lab to specialty care centers

The Department has an obligation through 252.12 and 252.13 to refer individuals with positive screening tests for early intervention and other appropriate services - if the disclosure is specifically for purposes of treatment and/or intervention, it would be allowable [253.12 (3)(a)1.d. and 253.13(4) & (5)]. Generally in Wisconsin, the disclosure is to the provider and patient family, not directly to specialty care centers except when the department is involved in a specific referral for treatment. A general disclosure to specialty care centers under Wisconsin law may require patient consent.

4. State lab to public health

The state lab discloses identifying patient information to state public health that then provides program assistance to physicians and patient families without requiring a patient authorization [Wisconsin Statutes 253.13 (5)].

5. Physician to state registry

There is an exception under Wisconsin Statutes 146.82(2)(a)5 that allows disclosure from the physician to the state agency upon receipt of a written request from the state agency. HIPAA 45 CFR 164.512.a and b allow disclosure by the physician to the state registry without patient authorization.

6. Public health to the patient's family

The state agency may notify the physician and the patient's families of eligibility for state programs however the patient/family may opt out of this notification [Wisconsin Statutes 252.13(3), (4) & (5)].

7. Physician to patient's family

State and federal law allow disclosure of information relating to positive screening test from physician to parents [Wisconsin Statutes 146.83 and 253.13 (4)]. Additionally, the patient (parent of minor) has legal right of access to their patient information under state and federal law [Wisconsin Statutes 146.83 and 253.14(5)1 and 45 CFR 164.524].

Other Wisconsin privacy laws allow disclosure to providers for treatment and to state agencies upon receipt of a written request [Wisconsin Statutes 146.82 (2)(a) 2 & 5].

Registry and Tracking

In addition to the disclosures of information, Wisconsin state law also requires the maintenance of a state registry of individuals with positive screening results [Wisconsin Statutes 253.12], in the form of a registry of children with birth defects [Wisconsin Statutes 253.12 (3)1.].

There is no requirement or continuing allowance for follow-up by the state registry to physician [Wisconsin Statutes 253.13(3)(a)1]. State law does allow for disclosure by a physician to a state agency that is doing a duly authorized function without a patient consent upon the receipt of a written request [Wisconsin Statutes 146.82(2)(a)5].

Documentation

HIPAA requires providers to document disclosures such that an accounting of disclosures is available to the patient [45 CFR 164.528]. Wisconsin Statutes 146.82(3)(c) requires documentation of disclosures made without informed consent. There is no state or federal law mandating or controlling documentation by the physician of receipt of the lab result.

The state lab is not required to verify the physician, as HIPAA Privacy and Security laws only require verification of requestor. There is no request made, so verification is not controlled by law.

Scenario 17 – Public Health Scenario C - Homeless shelters

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.

Variations Workgroup Summary:

Wisconsin law requires that special protections be observed and enforced for “sensitive” health information, including mental health, HIV test results, and developmental disabilities. These protections include more specific consideration for the information being disclosed (needs more detailed information) and a specific timeframe (e.g., only applies for 1 year). Sensitive health information requires more consent and documentation to release information, even for treatment purposes. Additionally, the interpretation of the legal requirements varies. Most agencies err on the side of being too protective of patient information so as not to incorrectly release information.

General information exchanged between the primary care provider and the drug addiction center for treatment purposes does not require patient consent. Some of our workgroup stakeholders would require consent for this exchange while others would not. In this scenario, the drug treatment center does not disclose to the primary care physician but that process in Wisconsin would require patient consent. Inconsistencies indicate variability in interpretation and application of state and federal law.

The addiction center could report treatment information back to the county for payment purposes without consent because the shelter is part of the county community services under chapter 51.

The disclosure to the relative requires a patient consent by law. However, some workgroup members felt that the information would be disclosed without consent if the shelter was not a covered entity.

As a result of more stringent requirements for security and privacy as well as the conservative interpretations of the legal requirements, an administrative burden is readily apparent for the treating organizations as well as complicating the implementation of an electronic record. In particular, there is disagreement on what constitutes a mental health record – the standard medications provided by a general practitioner or only the information collected by a mental health professional?

Consent and documentation of the release of information created the biggest barrier to the exchange of information. For purposes of sharing with the local public health department for payment or treatment purposes, there were limited barriers for the exchange of either identified or de-identified information.

A complicating issue in this scenario was the request for information from the shelter. Wisconsin had one health care organization that also operated a shelter, and would require a release. In general, though, the consensus was that the shelter would not view information about the patient's residence in a mental health facility (considered to be sensitive information in Wisconsin) to be health information. Therefore, it was believed that this information would typically be shared without consent from the patient.

Minimum necessary would not apply to information exchanges for treatment, however it would be appropriate to apply this standard to all other exchanges in this scenario and all stakeholders applied this standard to the information exchange.

Legal Analysis

Disclosure of patient information

The Legal Workgroup analyzed the following exchanges of health information related to this scenario:

1. Addiction center to county for program reimbursement

Wisconsin Statute 51.30(4)(b)2 allows disclosure of treatment information for payment purposes without patient consent to DHFS or a county department under s.51.42 or 51.437. The Federal Privacy Law allows disclosure without consent for payment purposes [45 CFR 164.506]. This disclosure would be allowed without consent under both state and federal law.

2. Addiction center to county homeless shelter

If the county shelter is providing community services under statutory authority,⁷⁴ the disclosure would be allowable without patient consent. If the county shelter does not have the appropriate statutory agreement with county services or DHFS, consent would be required. The Federal Privacy Rule allows disclosures between providers for

⁷⁴ Wis.Stat. 46.215, 46.22, 51.42 or 51.437 the disclosure would be allowable without patient consent. If the

treatment [45 CFR 164.506]. If the county shelter were not deemed a provider, consent would be required under federal law.

3. County shelter to relative

This disclosure would not qualify for release without consent under Wisconsin statute 51.30(4)(b) and a consent would be required. Federal privacy law both 42 CFR and HIPAA would require consent to the family. HIPAA would allow disclosure to the family if they were involved with the patient's care and the patient agreed, which are not applicable facts under this scenario.

Verification of requestor

Both state and federal law would require verification of the requestor for sensitive patient information in this scenario.

Transmission of information

The Federal Security Rule would require that any electronic transmission of patient information be secured under the statutory requirements.

Documentation of disclosure

HIPAA does not require documentation of disclosures for treatment and payment⁷⁵ but most other disclosures by a covered entity would be documented and accessible to the patient. Wisconsin Statute 51.30 requires documentation of disclosures made by a healthcare provider, so when applicable in this scenario, such as from the substance abuse facility, documentation would be required.

Minimum necessary

Federal law and Wisconsin law applicable to sensitive information require that the disclosure, for any purpose other than treatment, be limited to minimum necessary.

2.10.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 - Patient and provider identification
- 4 - Information transmission security or exchange protocols
- 5 - Information protection (against improper modification)
- 6 - Information audits that record and monitor activity
- 7 - Administrative or physical security safeguards
- 8 - State law restrictions
- 9 - Information use and disclosure policy

⁷⁵ 45 CFR 164.528(a)(1)(i)

1 – User and entity authentication

When receiving a request for health information, all relevant stakeholders stated that they would verify the requester prior to disclosing information, except in public health communities where the requestor would be known. Some stakeholders require additional information from the requester and may require the request to be sent on letterhead, by fax or mail.

In the case of mental health, as in Scenario 17, a written request for patient information would be required to indicate the information needed and to verify the requestor. If the necessary consent and treatment requirements were met, the information would be sent only by mail to the provider making the request, except in the case of emergency.

Verification practices are generally driven by federal law, which is more stringent than Wisconsin state law. Federal law states that requests need to be verified, but does not state how the verification should occur. State law does require verification of the requestor for requests related to mental health, alcohol and drug abuse and developmentally disabled. Among stakeholders queried for these scenarios, there is wide variation in verification practices.

All stakeholders listed employed the following:

- Nearly all stakeholders employ some form of physical identification within their organizations. Often the badges used contain authorization for accessing certain physical locations within the building. Restricted access can be in the form of hours of the day, physical location of medical information and isolation units that can be accessed. There is variation in how this method is used to limit authorization.
- A two-factor authentication process is employed for most electronic systems. For example, the DHFS Health Alert Network (HAN) requires a user ID and password. When access is established for this system, this information is used to define a person's role-based access.
- A patient identification number, in the case of the newborn scenario. This number is used to submit the mandated screening materials and to uniquely identify the patient when tracking the results.

2 – Information authorization and access controls

When receiving a request for health information, all relevant stakeholders stated that they would verify the requester prior to disclosing information, except in public health communities where the pool of those sharing the information is very small. Some stakeholders require the requester to send a request for information on letterhead, by fax or mail.

Nearly all stakeholders employ some form of physical identification within their organizations. Often the badges used contain authorization for accessing certain physical locations within the building. Restricted access can be in the form of hours of the day, physical location of medical information, and isolation units that can be accessed. There is variation in how this method is used to limit authorization.

Public health agencies do not typically have a way to limit physical access to their records, but typically are limited by function (i.e., the person responsible for the program is responsible for

securing the files). These agencies have access to locked file cabinets and the building is secured outside of regular business hours.

The stakeholders with electronic medical records have policies and procedures to limit access to read-only, modify information, or edit/delete information based on a user's role. For the most part, organizations with paper records have policies that clearly state who can modify patient records. The perception was that paper records are generally more difficult to modify, and more so when additional logging procedures are used to track changes to the record. The perception that paper records are more secure and the variability in practice in relation to authorization for modification and protection of data integrity may create barriers in information exchange.

3 - Patient and provider identification

The clinician sends identifiable patient information, including progress notes, to state agencies as requested on the state form (currently by mail). If the form is on state letterhead, the physician will disclose information without additional identifying information. Since the request for this information is regulated by state law the clinician will typically not question the nature of this kind of request.

The patient is typically identified through a number of data elements, including name, date of birth and address. In a medical care setting, this information is used to determine if the patient is under the care of a physician within its organization. When results are received, this information is used to match the patient with his/her file, and the results are incorporated.

The public health agency does not typically verify the clinician's identification when mandatory conditions are reported. Often there is a form that is used to follow up that requires more specific information from clinician, and his/her identity would be captured through this process.

The patient is typically identified through a number of data elements, including name, date of birth and address (or in the case of an electronic environment, information related to a master person index). In a medical care setting, this information is used to determine if the patient is under the care of a physician within its organization. When results are received, this information is used to match the patient with his/her file in both clinical and payment settings and the results are incorporated.

Law enforcement or local public health staff will often request a form of identification, such as a driver's license, when involved in removing someone with a communicable condition from public transportation.

4 - Information transmission security or exchange protocols

Information transmission occurs when a request is made for patient information. The Variations Workgroup found variability in how requests for patient information are made. Some send written requests for patient information by mail or via fax, and responses to these request are usually made in the form in which the request was received. If information is needed immediately, nearly all workgroup members would fax the information. Requests made over the phone are generally not documented.

By state law, extra care must be taken in transmitting sensitive health information. Generally this is only released for treatment purposes, and even then only the information relevant to the care being received. In the case of mental health, as in Scenario 17, a written request would be required indicating the information needed. If the necessary consent and treatment requirements were met, the information would be sent only by mail to the provider making the request, except in the case of emergency.

For the public health scenarios, the business practices documented center around the transmission of test results and treatment information to the parties entitled by law to receive them. This information is primarily released in verbal fashion or paper format, with the exception of newborn screening results which are made available to hospitals through a secure Web portal. Processing of mandated tests is handled through the state lab, which in turn relays test results to the appropriate parties.

When a physician provides the test results or treatment information to a patient and their family, generally s/he will schedule an appointment with the family and verbally relay the results. In the event that a primary physician cannot be identified, the local public health agency will be contacted to provide these results.

In the case of the need to communicate information about a communicable disease to a non-medical or public health professional, the minimum information necessary would be provided. Based on the circumstances, information about the event could be released to public health and medical professionals registered on the state's Health Alert Network (HAN) or individually to those that need this information. The information provided would include general information about the type, location, and nature of the event. Additionally, if this is deemed to be a broader public health concern, a written press release informing the public of the event would be provided to the press and posted on the public health Web sites. The method for providing this information to medical professionals, public health, and the public is determined on a case-by-case basis.

5 – Information protections (against improper modification)

The stakeholders with electronic medical records have policies and procedures to limit access to read-only, modify information, or edit/delete information based on a user's role. For the most part, organizations with paper records have policies that clearly state who can modify patient records. The perception was that paper records are generally more difficult to modify, and more so when additional logging procedures are used to track changes to the record. The perception that paper records are more secure and the variability in practice in relation to authorization for modification and protection of data integrity may create barriers in information exchange.

Policies and procedures are in place for appropriate handling of the records, including auditing functions. Variations exist in the implementation of these policies.

Information audits that record and monitor the activity of health information systems.

6 - Information audits that record and monitor activity

When information is released from one facility to another, stakeholders varied as to whether or not they logged the release. Typically if the information is processed through the medical

records clerks, the following information is logged: requestor name, facility/company, patient identification, date/time, and purpose. For sensitive information, even though documentation of the release is required by law, some would document and others would not.

For those who document the disclosure in a paper environment, the documentation can come in the form of a handwritten note in the patient's chart, a paper log, or inclusion of the release form or the form submitted to public health in the patient's chart. If the organization uses an electronic medical record, the technology would log who accessed the information, but would not log the specific circumstances surrounding the disclosure. In practice the stakeholders said that not every disclosure is documented.

The statutory requirements for documentation of disclosures, specifically under state law, were deemed onerous barriers to information exchange.

7 – Administrative or physical security safeguards

Public health agencies do not typically have a way to limit physical access to their records, but typically are limited by function (i.e., the person responsible for the program is responsible for securing the files). These agencies have access to locked file cabinets and the building is secured outside of regular business hours.

Nearly all stakeholders employ some form of physical identification within their organizations. Some organizations color-code badges to indicate the employing department of a staff member. Often the badges contain authorization for accessing certain physical locations within the building. Restricted access can be in the form of hours of the day, physical location of medical information, and isolation units that can be accessed.

The security of paper records is safeguarded by policies. Representative stakeholders stated that they have policies that records must remain in the building at all times, and are more restrictive for records containing sensitive information.

Public health agencies do not typically have a way to limit physical access to their records, but typically are limited by function (i.e., the person responsible for the program is responsible for securing the files). These agencies have access to locked file cabinets and the building is secured outside of regular business hours.

Policies and procedures are in place for appropriate handling of the records, including auditing functions. Variations exist in the implementation of these policies.

8 – State law restrictions

1. Obtain consent and determine which information to disclose
 - Scenario 15 - For public health to release information in the event of a communicable disease, information can be exchanged without consent, but is usually limited to the minimum information necessary. Even the process of obtaining consent varies based on the severity of the disease in question and the threat to the public at large.

- Scenario 16 - In the case of genetic testing, the release of information is mandatory, and the information required is defined at the state level and communicated through a standard form. The patients and their families are only provided the opportunity to opt out of the exchange after the initial test results have been provided to the physician.
- Scenario 17 – All stakeholders would require a consent form indicating the specific information to be released related to the patient’s treatment in a mental health facility, with the exception of providing information for payment purposes. One stakeholder said that the completed consent form would be provided to the appropriate caregiver in the mental health unit for review. Upon approval from the mental health provider, the information would be disclosed by sending a paper copy of the records with the patient to the treatment facility, mail, or fax (based on the circumstances).

In the event of a medical emergency, the requestor must declare the purpose of request as a medical emergency, whether verbally or in writing, which will be documented in the case file.

2. Documentation of Disclosure

Wisconsin state law requires documentation of the release of sensitive information from provider to provider for treatment purposes. Law does not dictate how the documentation needs to be made and therefore there are wide discrepancies in documentation practices. Stakeholders regard the state documentation requirements as onerous.

3. Re-disclosure

There are Wisconsin requirements for disclosing health information obtained from another provider. However, there is variability among stakeholders in the application of the law. The re-disclosure provision creates difficulties in determining what information may be disclosed from a patient’s record and therefore creates barriers to exchange.

9 – Information use and disclosure policy

1. Obtain consent and determine which information to disclose

- Scenario 15 - For public health to release information in the event of a communicable disease, information can be exchanged without consent, but is usually limited to the minimum information necessary. Even the process of obtaining consent varies based on the severity of the disease in question and the threat to the public at large.
- Scenario 16 - In the case of genetic testing, the release of information is mandatory and the information required is defined at the state level and communicated through a standard form. The patients and their families are only provided the opportunity to opt out of the exchange after the initial test results have been provided to the physician.

- Scenario 17 – All stakeholders would require a consent form indicating the specific information to be released related to the patient’s treatment in a mental health facility, with the exception of providing information for payment purposes. One stakeholder said that the completed consent form would be provided to the appropriate caregiver in the mental health unit for review. Upon approval from the mental health provider, the information would be disclosed by sending a paper copy of the records with the patient to the treatment facility, mail, or fax (based on the circumstances).

In the event of a medical emergency, the requestor must declare the purpose of request as a medical emergency, whether verbally or in writing, which will be documented in the case file.

2. Documentation of disclosure of patient information

For those who document the disclosure in a paper environment, the documentation can come in the form of a handwritten note in the patient’s chart, a paper log, or inclusion of the release form or the form submitted to public health in the patient’s chart. If the organization uses an electronic medical record, the technology would log who accessed the information, but would not log the specific circumstances surrounding the disclosure. While the practices stated above are the policies of the representative organizations, in practice all said that not every disclosure is documented/

3. Receipt of information into patient record

Stakeholders discussed a variety of ways that patient health information is incorporated into the medical record. These included placing the material in the chart following: the physician’s review and validation of the information by initialing, date and time stamping; and/or entry into a logging system; scanning by the medical records staff; and isolating the information in a separate section (for outside records) within the patient record.

2.10.4 Critical Observations

Unique to Wisconsin

Although Wisconsin law generally provided for disclosure without consent for public health purposes or health oversight, a consent is required for disclosures of sensitive information (mental health, alcohol and drug abuse and developmentally disabled) in several exchanges within these scenarios when a consent was not required by federal law.

Wisconsin requirements for documentation of disclosures related to the above more sensitive information were also often more stringent than federal as for treatment and payment.

Major Barriers to Exchange

Consent

In general both state and federal law allow for disclosure for public health and health oversight without patient consent.

Any time consent is required to exchange information, it creates a barrier to exchange. Differences in state and federal law regarding when consent is required and the required components of consent exacerbate the barrier.

Consents are required by law in Wisconsin for the exchange of sensitive information unless the disclosure meets one of the very specifically defined and rigid exceptions. The Wisconsin law is also more stringent than federal law, which results in barriers to exchange across state lines. The requirement of consent is driven by law and policy and poses barriers to information exchange.

Wisconsin law requires special protections be observed and enforced for “sensitive” health information, including mental health, HIV test results, and developmental disabilities. Additionally, the interpretation of the legal requirements varies creating additional barriers to exchange.

Documentation of disclosures

State regulations requiring the documentation of disclosures pose significant barriers to exchange. The requirements are rigorous and difficult to interpret and therefore there are variations in how the documentation is completed.

Verification of requester

Federal law mandates that the requester of health information be verified before health information is exchanged. Practices for verifying the requester vary and taking this additional step to verify the requester slows the exchange process.

Within several of these scenarios state law (mental health and alcohol and drug abuse) also require verification of the requestor presenting additional barriers to information exchange.

Minimum necessary

Typically, the minimum amount of information necessary is provided, but whenever the public’s health is at stake, more comprehensive personal health information may be provided. Federal requirements to limit the exchange of health information to minimum necessary increase the amount of time required to exchange health information. Often technology cannot limit disclosures to the minimum necessary, so processes that could be electronic are manual in order to limit the information disclosed. For organizations with paper records, sifting through records to make sure that the minimum necessary is exchanged is also time consuming, creating a barrier to exchange.

Re-disclosure requirements

State law has specific requirements for re-disclosure of health information. Not only is a barrier created by the requirements themselves, but varying interpretations of the law create inconsistent application and therefore a barrier to exchange. This legal requirement would apply when information is released from the substance abuse facility to the county homeless shelter and then requested by the relative.

Request for information practice

The variability in the process used for making the request for patient information - by phone, in writing, by fax, when linked with specific requirements for the format of requests creates barriers to efficient exchange of patient information.

As a result of more stringent requirements for security and privacy as well as the conservative interpretations of the legal requirements, an administrative burden is readily apparent for the treating organizations as well as complicating the implementation of an electronic record. In particular, there is disagreement about what constitutes a mental health record – the standard medications provided by a general practitioner or only the information collected by a mental health professional?

Consent and documentation of the release of information create the biggest barrier to the exchange of information in these scenarios. For purposes of sharing with the local public health department for payment or treatment purposes, there were limited barriers for the exchange of either identified or de-identified information.

2.11. State Government Oversight (Scenario 18)

2.11.1 Stakeholders

The following stakeholders from the Variations Workgroup provided input for the discussion of the state government oversight scenario:

- Public health agencies
- State government
- State university faculty

Please refer to section 1 for a detailed description of the stakeholders.

2.11.2 Summary of Findings

This section contains the scenario followed by the high level finding of the Variations and Legal Workgroups.

Scenario 18 – Health Oversight: Legal compliance/government accountability

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

Variations Workgroup Summary

Patient identifiable information would not be disclosed to faculty at a state university without a business agreement. The state agency can share this information between agencies, but cannot send the information to a state university faculty without a business agreement.

Legal Analysis

Consent would not be required for disclosures among state agencies with statutory authority to collect patient information and statutory authority to use that patient information for a legally authorized function.

This scenario asked that agencies share identifiable patient level information, including Medicaid Services to determine if the children are getting the healthcare they need. However, a potential barrier exists which involves the disclosure of Medicaid Data. Both federal and state law (Wis. Stat. §49.45(4)) do not allow DHFS to disclose identifiable information about recipients

enrolled in the Medicaid Program unless the disclosure is for the administration of the Medicaid Program. In this scenario, the intent of the disclosure is not really clear based on the information provided. An analysis would need to be completed prior to the release of this information.

Disclosures of patient identifiable information between state agencies and a state university for the purpose of building a data bank for the state would require patient consent or a legally authorized business associate agreement. This disclosure would be regulated by the HIPAA Security and Privacy Rules and require a business associate agreement between the entities to share/exchange identifying patient information.

Another barrier is if the disclosure of the Medicaid Data has been determined to be used for the purposes of the administration of the Medicaid Program, the data cannot be disclosed unless there is a business associate agreement in place between the University and the Department, otherwise the disclosures cannot occur as this is a requirement within the federal privacy regulation.

HIPAA would also require verification of the requestor for health information, a secured electronic transmission and the application of the minimum necessary standard for disclosure (unless for treatment).

2.11.3 Domains

The Variations Workgroup identified the following domains as relevant to this scenario:

- 1 - User and entity authentication
- 2 - Information authorization and access controls
- 3 - Patient and provider identification
- 4 - Information transmission security or exchange protocols
- 5 - Information protection (against improper modification)
- 6 - Information audits that record and monitor activity
- 7 - Administrative or physical security safeguards
- 8 - State law restrictions
- 9 - Information use and disclosure policy

1 - User and entity authentication

To verify the requestor, the Governor would request that the agencies share this information both verbally and in person. The in-person request would come through the chain of command. Requiring an in person request would be a barrier to HIE. (Note: It is very unlikely that the Governor's office would request this information be shared.)

2 - Information authorization and access controls

For physical security measures, the business associate agreement and/or data use agreement will specify a means for providing secure access to users in an electronic environment, based on functionality or role (e.g., key card access).

3 – Patient and provider identification

The patient is typically identified through a number of data elements, including name, date of birth and address (or in the case of an electronic environment, information related to a master person index).

4 - Information transmission security or exchange protocols

Provided there was a business associate agreement (commonly referred to as a data use agreement when utilized by state agencies) in place, state agencies would provide non-sensitive health information to the contractor for compliance purposes in an electronic format. The requirement of a business associate agreement is defined and regulated by federal law. The agreement would be required to meet all the statutory requirements and often a data use agreement unless in compliance with federal law would not be sufficient. The stakeholder described the agreement as generally providing role-based access to the database or access through an extract file on CD. Also, a secure database would be provided with manipulated data, which the research agency would import into a secure environment.

5 – Information protection (against improper modification)

Provided there was a business associate agreement (commonly referred to as a data use agreement) in place, state agencies would provide non-sensitive health information to the contractor for compliance purposes in an electronic format. This would be done by providing role-based access to the database or through an extract file on CD. Also, a secure database would be provided with manipulated data, which the research agency would import into a secure environment.

6 - Information audits that record and monitor activity

In order to document disclosure of patient information, the business associate agreement and/or data use agreement will specify a means for providing secure access to users in an electronic environment, based on functionality or role. This electronic environment will provide an audit function.

7 - Administrative or physical security safeguards

Public health agencies do not typically have a way to limit physical access to their records, but typically are limited by function (i.e., the person responsible for the program is responsible for securing the files). These agencies have access to locked file cabinets and the building is secured outside of regular business hours.

In order to document disclosure of patient information, the business associate agreement and/or data use agreement will specify a means for providing secure access to users in an electronic environment, based on functionality or role.

The information would not be disclosed to the contractor from state agencies without a business agreement in place to regulate the use of the data provided.

8 – State law restrictions

Medicaid

The state Medicaid law restricts the disclosure of state Medicaid data and although use within the state agency would be allowable for a legally authorized function, disclosure to the state university would not be allowed without a business associate agreement.

Consent

Wisconsin privacy law allows disclosure between state agencies doing a legally authorized function without patient consent. Wisconsin law requires a patient consent or a legally authorized contract for services such as a business associate agreement to allow disclosure from the state agencies to the state university⁷⁶

Documentation of disclosure

Wisconsin law requires that any agencies meeting the definition of health care provider document any activities deemed disclosures.

9 - Information use and disclosure policy

Provided there was a business associate agreement (commonly referred to as a data use agreement) in place, state agencies would provide non-sensitive health information to the contractor for compliance purposes in an electronic format.

The research agency would not access or use the non-sensitive health information until a business associate agreement/data use agreement regulating the use of the data into the database was completed.

2.11.4 Critical Observations

The stakeholders did not feel that a request, as described in this scenario, would occur in Wisconsin. The stakeholders anticipated that the level of business associate agreements/data use agreements necessary for this scenario to occur would be prohibitive, and therefore this exchange of data would not occur.

Although this scenario would not be anticipated to occur in Wisconsin, the stakeholders attempted to identify the business practices that would occur for this type of exchange of information

It is unclear whether consent would be required for all populations, as this scenario covers a very broad range of stakeholders (i.e., schools, Medicaid, public health, etc.).

⁷⁶ 146.82(a)

Unique to Wisconsin

The state Medicaid laws restrict disclosure of Medicaid data, a regulation that would present a barrier to information exchange. Federal law does not provide for this more stringent restriction within this scenario.

Wisconsin law also requires that any of the state agencies defined as covered entities or health care providers document any activities relating to health information exchange that might be deemed a disclosure.

Major Barriers to Exchange

Business associate agreement

This exchange would require a business associate agreement/data use agreement under both state and federal law. Meeting the statutory requirements for that agreement in this scenario might be onerous and present a barrier to information exchange.

Secured transmission and storage

For this exchange, it may be necessary for data to be provided in a separate, secure database, to ensure the integrity of the original data, and to allow for manipulation of identifiable information. This secured protection would present a barrier to information exchange.

Federal law

HIPAA would also require verification of the requestor for health information, a secured electronic transmission and the application of the minimum necessary standard for disclosure (unless for treatment). All processes presenting a barrier to open information exchange.

Consent

Wisconsin state and federal law require patient consent to disclose the information to the state university unless a business associate agreement is in place. State and federal requirements for consent vary and therefore most consents produced in Wisconsin satisfy both requirements. Both the obtaining consent and the requirements of the consent specific to Wisconsin serve as barriers to exchange.

Documentation of disclosure

Wisconsin state law requires documentation of the disclosure of information to the state university unless a business associate agreement is in place and the exchange is considered a use. While compliance with the documentation requirements vary, the requirements to document the release of information pose a barrier to exchange.

3. Summary of Critical Observations and Key Issues

A barrier to health information exchange (HIE) is defined as a business practice or policy that may impede access to health information or health information exchange despite what the law does or does not allow.

The Variations and Legal Workgroups analyzed the 18 scenarios distributed by RTI. The scenarios assisted the Variations Workgroup in identifying business practices driven by practice, policy or law that may create barriers to health information exchange. Variation in business practice creates additional barriers to HIE because methods used to perform tasks associated with the exchange of information vary.

Legal barriers also exist at both the state and federal level, which limit the ability to exchange health information. Furthermore, varying interpretations of statutory regulations create variations in business practices, which in turn create additional barriers to HIE.

This section summarizes the barriers identified by both the Variations and Legal Workgroups and will serve as a starting point for the Solutions Workgroup.

3.1 Barriers driven by state and federal law

A legal barrier to HIE is a statutory or regulatory requirement that prevents the free flow of health information.

During the legal analysis of state and federal law, the Legal Workgroup identified that Wisconsin law has privacy provisions that protect what is commonly referred to in Wisconsin as “sensitive” patient information. Generally this term refers to patient information that is protected more stringently than other patient information under state and/or federal law. Within the guidance of Wisconsin Law, this “sensitive” information that is protected more stringently under state law includes mental health, alcohol and drug abuse, developmentally disabled and HIV test results. Wisconsin Statute 51.30 regulates mental health, alcohol and drug abuse and developmentally disabled patient information. Wisconsin Statute 252.15 regulates the confidentiality of a patient’s HIV test result. Both these statutes provide more stringent protection than other privacy laws although the statutes differ in the protection they provide. This complexity provides insight into the difficulties faced when interpreting state law, federal law and the interface between state and federal law.

The scenarios helped the workgroups to identify several legal barriers, both state and federal, which greatly impede health information exchange. We will first highlight the legal barriers that are unique to Wisconsin state law, then those posed by both state and federal law and finally the barriers posed solely by federal law.

3.1.1 Barriers driven by Wisconsin state law

Treatment of Mental Health, Alcohol and Drug Abuse and Developmentally Disabled information
Wisconsin state law treats information relating to mental illness, developmentally disabled or alcohol and drug abuse as “sensitive” and provides more stringent privacy protection. Any health record that contains this type of information and meets the statutory definition for

protection requires patient consent to disclose for treatment or payment purposes. Federal law allows these disclosures for treatment purposes without a consent, which creates more of a state barrier to national exchange because our state has different regulations than federal law and other states. Furthermore, because generally, current technology cannot limit access to a portion of a medical record in most cases, this more stringent protection severely limits information exchange. Finally, the consent must meet the statutory requirements for a valid consent under Wisconsin state law, which further increases the barrier because the elements differ from federal law and likely from required elements in other states.

Treatment of HIV Test Results

Wisconsin state law also treats HIV test results as “sensitive” information and provides more stringent privacy protection. Although Wisconsin law allows the exchange between providers without patient consent for treatment purposes, consent is required for payment and other disclosures that under federal law do not require consent. The technical problems associated with the ability to limit or control access exemplified with the above sensitive information are also present in the disclosure processes associated with the HIV test result and also present legal barriers to health information exchange.

Documentation of disclosures

Wisconsin state law requires the documentation of all disclosures made with or without patient consent. Documentation requires several elements that vary slightly if the information is sensitive or non-sensitive. In practice, compliance with the law varies, however our stakeholders each stated that the requirements pose a significant barrier to exchange. The stakeholders did feel that with technological advances, documentation of disclosures could be automated, eliminating this part of the barrier.

HIPAA does not require documentation when the exchange is for treatment purposes. In addition to the documentation requirements, the discrepancy between Wisconsin and federal law serves as a barrier to exchange.

Verification of the requester

Wisconsin state law mandates verification of the requestor of health information related to mental health, alcohol and drug abuse and developmentally disabled and does not require verification for the disclosure of general health information. The law does not indicate how the verification process should occur and therefore, verification practices vary. The requirement to verify the requester slows down the exchange of information, as does the wide variation in verification practices.

Re-disclosure requirements

State law has specific requirements that prohibit re-disclosure of general health information released without patient consent. Not only is the prohibition on re-disclosure a barrier created by the requirements themselves, but varying interpretations of the law create inconsistent application and therefore a barrier to exchange.

Private pay patients opt out of research

Recognizing the benefits of controlled and secured research processes to patient care, there are currently patient privacy statutes that allow private pay patients to opt out of research projects. This process may ultimately result in a barrier to information exchange for research purposes.

3.1.2 Barriers driven by state and federal law

Consent

Any time a consent is required to exchange information, it creates a barrier to exchange. The process to obtain a consent poses a barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. It requires determining who is legally authorized to sign the consent and it requires validating the statutorily required elements of the consent.

The consent process requires interface between state and federal law to determine which law controls in determining whether a consent is required and the required elements in the consent because state and federal requirements are different. In practice, most consents contain both the state and federal requirements which may cause confusion in the validation of the consent. In addition, the requirements for consent may change when crossing state lines and a Wisconsin consent may not be valid in another state and visa versa.

Lack of statutory definitions

In many cases, laws exist to protect the privacy of patient information, but because the definitions are unclear, they are open to wide discrepancies in interpretation. This results in wide variation in business practices, which, in turn, leads to barriers of health information exchange because of the variation.

For example, there are differences among stakeholders in defining a disclosure and therefore determining whether or not documentation of the disclosure is required. There are also differences in defining the elements of an informed consent for release, resulting in a variety of approaches to verifying a patient consent that may ultimately lead to a denial of exchange.

3.1.3 Barriers driven by federal law

Verification of requester

Federal law mandates that the requester of health information be verified before health information is exchanged. Practices for verifying the requester vary and taking this additional step to verify the requester slows the exchange process. Furthermore, the law does not give guidance as to how to perform verification, so practices are variable, which creates additional barriers to exchange information.

Minimum necessary

Federal requirements to limit the exchange of health information in certain types of disclosures to the minimum necessary standard and only release what is necessary to fulfill the request,

increase the amount of time required to exchange health information as well as the ability to receive comprehensive records. Often technology cannot limit disclosures to the minimum necessary, so processes that could be electronic need to be manual so that the information can be manually limited. For organizations that use paper records, sifting through records to make sure that the minimum necessary is exchanged is also time consuming, creating a barrier to exchange.

Variability in how the standard applies creates an additional barrier. What one health care provider may determine to be minimally necessary may vary greatly from that defined by another. In addition, several stakeholders applied the minimum necessary standard to internal disclosures and others did not. This variability in the application of the minimum necessary standard may present a barrier to information exchange and ultimately to patient care.

Business associate agreements

The federally mandated requirement of an extensive and legally sound business agreement to allow exchange between a covered entity and a company using protected health information to do business may cause a barrier to information exchange.

The creation of a business associate agreement that meets the needs of both the provider and the vendor can present a conflict in the protection of information. (federal law)

Transmission of healthcare information

The Federal Security Rule requires that covered entities implement technical security measures to guard against unauthorized access to electronic protected health information that is transmitted over an electronic communications network. Although the federal law allows flexibility in compliance with this standard, this level of security is often difficult for some electronic systems to meet, thereby creating a barrier to health information exchange.

Uses vs. Disclosures

Wisconsin state law does not regulate what it considers uses of information that are not disclosures. These are often internal exchanges where information is simply used to perform an internal business function. Federal privacy law does however regulate the use of protected health information. The federal regulation imposes additional protections and restrictions that create legal barriers to information exchange in Wisconsin. The additional regulation specifically of internal use of creates a barrier to information exchange. In the scenarios, in cases where Wisconsin state law would not regulate an internal use, federal law would be followed. The additional federal restrictions create barriers to information exchange in Wisconsin.

3.2 Barriers driven by policies and practices

Consent

Some stakeholders have policies requiring patient consent for disclosure that are more restrictive than state or federal law. For example, most stakeholders have policies requiring consents for disclosure of HIV test results for treatment purposes, even though the law allows this exchange without patient consent.

Additionally, some organizations have policies that do not allow the internal exchange of information without patient consent. Because it does not often make sense to obtain patient consent when exchanging information internally (to send marketing materials to a patient), the policy requiring patient consent effectively stops all internal exchange of information in these cases and presents a major barrier to health information exchange.

Method of requesting information

There were significant variations in the methods used for making a request for patient information, including phone, fax and in writing. This variability when linked with specific requirements for verification of the requestor results in barriers to efficient exchange of patient information.

Request for information practice

There is significant variability in the format used or required to be used for making requests for patient information - in writing, by fax, on letterhead, or with a consent. This variability creates barriers to efficient exchange of patient information.

Method of disclosure

The method of disclosure varied greatly among the stakeholders from fax, phone, mail and electronic exchange. The various methods also exemplified the use of various processes for exchange, many lacking security measures during transfer of information. Many stakeholders preferred a paper copy sent by mail over electronic exchange to remove the responsibility for security.

Technology

All of the stakeholders with EMRs who stated they would not allow external access to their health records, stated they would allow access if their technology allowed them to limit access to only relevant parts of the record and only to specific records to comply with minimum necessary requirements. Furthermore, current technology cannot specify the type of access that is granted. The stakeholders were unable to identify a way to grant read-only vs. update access or to audit what information is retained by the payer. For those who use electronic medical records, the technology itself creates a barrier to exchange. For those who do not have electronic medical records, paper records themselves create a barrier to exchange.

3.3 Opportunities

Changes in law

Many of the barriers identified by the Variations and Legal Workgroups were driven by state and federal laws. There are many regulations in place to protect patient privacy that impede the exchange of information and in many cases good patient care. When information is not exchanged freely, providers are forced to make decisions without full information.

The Variations and Legal Workgroups understand that while some of the privacy restrictions are necessary to protect consumers, the Solutions Workgroup can analyze current legal restrictions and make recommendations as to which laws create barriers that are truly necessary to protect patient privacy and which are simply an impediment to patient care.

Laws which vary between state and federal law should be re-examined. If information is to be exchanged across state lines, state laws should mirror federal standards. If state laws are less restrictive than federal laws, then in some cases our workgroup would recommend changing federal law to match state law. The Solutions Workgroup should examine the areas where state and federal law differ and make recommendations.

Changes in policy and procedure

Many of the barriers identified by the Variations and Legal Workgroups were driven by policy and procedures or established business practices. Clarification of the privacy laws may assist in a clearer understanding of the rules and regulations. The variability identified in policies and practices offers the Solutions Workgroup an opportunity to explore model policies and procedures for health information exchange that will assist in standardization of “good practices” and consistency in disclosure processes.

Improvements in Technology

In many cases, barriers to HIE would be eliminated with advances in technology and our group believes that without advances in technology, we cannot have effective HIE.

First, many organizations do not use electronic medical records currently. Often systems are too expensive and do not fill the needs of the organization. Without universal adoption of electronic medical records, technology will always pose a barrier to exchange.

Secondly, automation of cumbersome business practices could serve to both decrease variability in business practice and eliminate the barriers posed by time consuming practices. For example, if documentation processes were automated, the barrier posed by those regulations could be effectively eliminated.

4. Appendices

By clicking on the icon provided below, you will be directly linked to the Excel spreadsheet that was used to collect the business practices for each scenario.



Business Practices by
Scenario