Wisconsin Security and Privacy Project

Assessment of Variation and Analysis of Solutions 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 53703

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

Submitted to:

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

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

March 30, 2007

Table of Contents

Executive Summary

In November 2005, by Executive Order #129, Governor Doyle created the eHealth Care Quality and Patient Safety Board (eHealth Board). The goal of the eHealth Board is to have 100% adoption of electronic health records systems and the appropriate exchange of health information from these systems within five years. The eHealth Board was charged with developing a roadmap for achieving this goal.

The eHealth Board submitted the Wisconsin *eHealth Action Plan* to the Governor in December 2006. This plan addresses the following challenges:

- Ensuring health information is available at the point of care for all patients.
- Reducing medical errors and avoiding duplicative medical procedures.
- Improving coordination of care between hospitals, physicians and other health professionals.
- Furthering health care research.
- Providing consumers with their health information to encourage greater participation in their health care decisions.

A key concern identified in the *eHealth Action Plan* is the requirement to exchange health information electronically in a way that is secure and protects a patient's privacy. In March 2006, the Department of Health and Family Services (DHFS) applied for the Health Information Security and Privacy Collaboration (HISPC) contract on behalf of the eHealth Board; the resulting effort is referred to as the Wisconsin Security and Privacy Project. Wisconsin was one of 34 states and territories awarded a contract to assess the security and privacy issues related to ehealth.

The Wisconsin Security and Privacy Project began in the fall of 2006 with the formation of four workgroups: Variations, Legal, Solutions, and Implementation. In the development of the four workgroups required by this project, Wisconsin was fortunate to have 52 individuals who volunteered their time, representing advocates, clinics, consumers, corrections, health care organizations, health care providers, health care quality organizations, hospitals, industry, laboratories, pharmacies, professional associations, public health, schools, payers, and state government.

Assessment of Variation

As required by the HISPC contract, the first group convened in this process was the Variations Workgroup. The Variations Workgroup was charged with reviewing 18 scenarios developed by RTI to identify current business practices related to health information exchange as well as the driver for each business practice. The Workgroup discussed variations in business practices between the responding stakeholders as well as which business practices posed barriers to health information exchange. For business practices which are considered barriers to exchange, the Workgroup discussed which barriers should remain as a privacy protection and which could be reduced or eliminated without removing necessary privacy protections. Staff assisted in the review of the business practices and the determination of which practices related to the domains in information exchange as identified by RTI.

The Legal Workgroup was convened shortly following the Variations Workgroup to identify the legal drivers of the business practices identified by the Variations Workgroup and evaluate potential legal barriers to health information exchange. The Legal Workgroup reviewed the 18 scenarios, and identified and cited the legal drivers for business practices as well as all legal barriers associated with the scenarios.

A summary of the barriers documented and analyzed by the Variations and Legal workgroups follows:

1. Barriers driven by Wisconsin law

Wisconsin statutory requirements relating to health information exchange (HIE) that are more restrictive than federal requirements cause barriers to the exchange of information.

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

- Consent for specific types of disclosures (payment and treatment)
- Verification of the requestor for this information
- Minimum necessary

HIV test results are also treated as sensitive information (Wisconsin Statutes section 252.15), except that they can be disclosed from provider to provider for treatment purposes.

Other barriers driven by Wisconsin law include:

- Documentation of all disclosures made with or without patient consent, including as defined in Wisconsin Statutes chapter 146
- Requirements prohibiting re-disclosure of health information
- Consent requirements more stringent than federal requirements, such as for disclosure to the patient's family
- Required interface between state and federal law requirements

2. Barriers driven by state and federal law

Whenever state and federal law do not mirror one another, several barriers to the exchange of information are created. First, one must determine which law controls (state or federal), then once the controlling law is determined, one must understand the requirements of the controlling law. This makes inter-state exchange of information increasingly difficult because other state laws must be understood in order to exchange.

Consent requirements, governed by state and federal law, present the greatest hurdles to health information exchange. 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
- Analysis required of state and federal law to determine which law controls
- Variation in requirements between states

Although eliminating these consent requirements would reduce the barriers to exchange, federal law 42 CFR Part 2 requires patient consent to exchange alcohol and other drug abuse information for treatment purposes unless revision of that federal law occurs.

Other areas where state and federal law differ include:

- Minimum necessary

- Verification of requester
- Requirement to provide of Notice of Privacy Practices

3. Barriers driven by federal law

In some cases, 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 identified by the workgroups that pose barriers to exchange include:

- Verification of the individual requesting the information.
- Release of the "minimum necessary" health information for the purposes identified by the individual requesting the information.
- Implementation of business associate agreements to govern the exchange of information that meets the needs of both the covered entity and the vendor.
- The Federal Security Rule, which governs the technical security measures to guard against unauthorized access to electronic health information.
- The Federal Privacy Rule requirements, including patient rights.
- Regulation of the use of protected health information in situations where the use would not specifically be deemed a disclosure, such as when information is used to perform an internal business function.

4. Barriers driven by policies and practices

The Variations and Legal workgroups identified several barriers to HIE that are driven by organization-level business policies and practices. Most often, variations in policy and practice implementation create 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
- Method of retention
- Variability of implementation of the law
- Method for making or responding to a request, such as by phone, by fax, or in writing.
- Sophistication of the technology that an organization is willing to purchase to secure its patients' information.

The final barrier to exchange identified by the workgroups is technology. In general, current technology used in Wisconsin cannot limit access to relevant parts of the record or to specific records to comply with "minimum necessary" requirements. Furthermore, currently employed technology often cannot 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. This will not be an easy barrier to overcome as technology systems are extremely expensive and many providers cannot afford the cost of technology. In addition, the costs related to the implementation of technology were also deemed a significant barrier to exchange.

Assessment of Solutions

Solutions Workgroup

The Solutions Workgroup was charged with the analysis of identified barriers, balancing privacy protections against the need to know and developing solutions to improve the exchange of health information. The Solutions Workgroup included a mix of members from the previous workgroups, as well as new members who increased representation in advocacy and policy making, for a total of 35 members. Members represented clinics, hospitals, consumer organizations, law enforcement, health care quality organizations, industries, pharmacies, professional associations, providers, public health, research, state government, health information vendors and payers.

The Solutions Workgroup reviewed barriers to health information caused by variations in organization-level business practices and relevant state and federal laws as identified by the Legal and Variations workgroups. The Solutions Workgroup followed a complex, creative approach that included a series of small breakout groups and large group discussions to allow active participation from all members, the capture of varied viewpoints, and ultimately the creation of solutions that will improve HIE without compromising necessary patient privacy protections. Through this process, each barrier was analyzed to determine whether it should remain or be reduced or eliminated. Solutions were developed to reduce or eliminate barriers that the group decided should not remain, and finally grouped into broader solutions with a greater feasibility of implementation.

Summary

An overview of the proposed solutions is provided below.

1. Verification of Patient

Currently, health care providers do not use a uniform method to capture standardized criteria to identify a patient (patient identifiers).[1,2] Moreover, there is not a standard method to verify patient identifiers at the time of exchange.[3] This lack of standardization creates significant risks to accurate and timely patient care. Variation in practice also poses a number of challenges to exchanging information in a paper or electronic format. Moving into an electronic world where information is exchanged between electronic health care systems will require standardized collection of patient identifiers, verification of patient identifiers, and accurate matching of identifiers to patient information. Currently, national efforts are under way to develop a set of unique patient identifiers to alleviate these issues.

The solution proposed by the Solutions Workgroup addresses current issues with misidentification of patients while positioning Wisconsin to incorporate the national recommendations once they are completed.

The Solutions Workgroup proposed the development of a standard set of identifiers as well as a set of model policies and procedures to ensure appropriate capture and verification of those identifiers. The project team would maintain an understanding of national efforts to develop a national set of identifiers, and develop policies and procedures that will accommodate the national recommendations. This way Wisconsin's model policies and procedures can be easily revised to incorporate national standards once they are established.

[1] Capture: The process of collecting patient identifiers from a patient.
[2] Patient Identifiers are information collected from a patient to assist in the identification of the patient (e.g., name, birth date, address, etc.)
[3] Verification: The process of confirming that patient identifiers are correct.

2. Modification of Wisconsin Statutes chapter 146 to mirror HIPAA in specific areas

Many of the barriers to health information exchange result from strict privacy protection requirements in the Wisconsin privacy laws. While some of the restrictions clearly interfere with or prohibit information exchange, others are so complex in their application that they result in wide variation in practices relating to disclosures. Additional barriers are created because HIPAA creates privacy protections in many of the same areas as Wisconsin Statutes section 146.81-146.84; thus application of these laws is complicated because it is difficult to determine which law applies.

Based on a review of the barriers to HIE created by the Wisconsin Statutes chapter 146, the Solutions Workgroup proposed revising this statute to mirror the language in HIPAA in the following areas:

1. Expanding disclosures to family (Wisconsin Statutes section 146.82, 146.83)
2. Expanding disclosures to law enforcement
3. Modifying re-disclosure restrictions (Wisconsin Statutes section 146.82(2)(b))
4. Modifying the requirements for documentation of disclosure (Wisconsin Statutes section 146.82 (2) (d), 146.83(3))

The Solutions Workgroup determined that these additional restrictions did not significantly improve patient privacy; instead they added to the complexity of health information exchange, which can result in individuals not having the information required to diagnose, treat or care for patients.

3. Modification of Wisconsin Statutes section 51.30 to allow the exchange of health information for treatment purposes

Wisconsin Statutes section 51.30 provides additional protections for health information that contains information related to mental health, developmental disabilities, and alcohol and other drug abuse. These additional protections create barriers to the exchange of information, some of which are arguably necessary privacy protections, while others, it can be argued, deter the exchange of information that could lead to better care. Additional barriers are created because Wisconsin Statutes section 51.30 is more restrictive than HIPAA regarding the exchange of information protected by this law.

The Solutions Workgroup reviewed barriers associated with these restrictions and determined that Wisconsin Statutes section 51.30 should comport with HIPAA and be revised to allow exchange of information between providers for treatment purposes, without patient consent. While this would allow the exchange of information protected by this law, it would not affect the provider's inability to disclose treatment information without patient consent protected by 42 CFR Part 2, the federal statute protecting AODA information. Consent would still be required to exchange this information.

It should be noted that the majority of the members of the Implementation Workgroup further refined the solution and determined that the law should be revised to allow the exchange of information for treatment purposes, but did not determine what information should be exchanged freely without consent.

4. Changes to HIPAA

The Solutions Workgroup reviewed all of the barriers associated with the HIPAA Privacy Rule that were identified through the Variations and Legal workgroups' review of the 18 scenarios. Following

discussions of the barriers, the Solutions Workgroup proposed changes to HIPAA in the following three areas:

a. Remove the requirement for a business associate agreement, and instead develop a method to hold business associates accountable for adhering to state and federal privacy requirements.
b. Remove the waiver process for research without patient consent, but maintain the Institutional Review Board (IRB) process requirements.
c. Clarify the "minimum necessary" standard by revising the language in HIPAA and developing model policies and procedures to define and clarify the standard.

This proposed solution was not reviewed by the Implementation Workgroup because it was determined that a plan to implement changes to federal law would most efficiently and effectively be created by individuals experienced with national legislative change.

Next Steps

The eHealth Board extends its sincere appreciation to all of the volunteers who dedicated their time to the Security and Privacy Project. The information that has been collected through this process will be valuable as the eHealth Board begins the implementation phase in developing electronic systems and a means to exchange health information electronically.

The recommendations contained in the report represent possible solutions to the challenges identified through the analysis of the 18 scenarios. The recommendations are intended to inform policy discussions, but should not be construed as comprehensive or definitive legislative recommendations of the eHealth Board at this time. The eHealth Board will be using the Security and Privacy Project reports to assess where the proposed solutions fit within the eHealth Board's scope of work for the coming years. Wisconsin is committed to developing the necessary policies and procedures to ensure the adoption of health information technology and exchange throughout Wisconsin in an effort to ensure quality of care and patient safety.

Section 1 - Background

1.1 Purpose and scope

The purpose of this report is to identify the variations in business practices that create "barriers" in exchanging health information and to identify potential solutions. "Barrier," as used in this document, refers to any policy or practice that hinders the exchange of health information without judgment as to whether the policy or practice is essential in ensuring patient privacy.

The process to develop these solutions included convening the following workgroups:

- Variations Workgroup: To conduct an analysis of organization-level business policies and practices that exist in health care settings across the state. From this Workgroup, a list of barriers were identified that the Workgroup believed hinder the process of exchange without providing any additional protections for patients.
- Legal Workgroup: To identify the legal citations that govern the policies and practices identified by the Variations Workgroup.
- Solutions Workgroup: To propose solutions to security and privacy issues that present challenges to the implementation of health information exchange.

The solutions developed by the Solutions Workgroup focus on barriers that exist in exchanging health information for treatment purposes.

Nearly all the barriers identified during the assessment process were presented to the Solutions Workgroup for consideration; representatives from all stakeholder groups participated in the meetings. In order to include representatives from all stakeholder groups, and keep the membership at a manageable level for the Solutions Workgroup meetings, several participants served more than one role. A limitation to this approach was that the Workgroup was dominated by hospital staff, legal experts, and professional associations.

1.2 HIT development in Wisconsin

By Executive Order in November 2005, Wisconsin Governor Jim Doyle created the eHealth Care Quality and Patient Safety Board. The goal of the Board is to have 100% adoption of electronic health records systems by health care providers and the appropriate exchange health information from these systems within five years.

The eHealth Board submitted the Wisconsin *eHealth Action Plan* to the Governor in December 2006. This plan addresses the following challenges:

- Ensuring health information is available at the point of care for all patients.
- Reducing medical errors and avoiding duplicative medical procedures.
- Improving coordination of care between hospitals, physicians and other health professionals.
- Furthering health care research.
- Providing consumers with their health information to encourage greater participation in their health care decisions.

In the process of developing the *eHealth Action Plan*, the eHealth Board conducted research in the areas of current technology and health information technology (HIT) adoption in Wisconsin. The following information regarding HIT development was taken from the *eHealth Action Plan*.

There is much work under way in Wisconsin, led by health care provider organizations, physicians, public health, technologists, scholars, and public and private health care purchasers. Many large health systems are already moving ahead with electronic health records and related investments. The Wisconsin Collaborative for Healthcare Quality, the Wisconsin Health Information Organization, the Wisconsin Medical Society and the Wisconsin Hospital Association, major insurers and provider organizations are collaborating on these efforts.

In 2005, MetaStar surveyed Wisconsin primary care practices, supplemented the results with field staff knowledge and identified that 38% of primary care practice sites in Wisconsin boasted an EMR.[4] In addition, two studies recently examined hospital HIT adoption in Wisconsin. Wisconsin has several well-established, integrated health care delivery networks with extensive HIE infrastructure in place. In 2005 MetaStar and the Wisconsin Hospital Association examined adoption of two technologies: Computerized Physician Order Entry (CPOE) and Telemedicine.[4] Of those responding to the survey, 82% are planning or considering CPOE and 33% are planning Telemedicine; 12% have partially implemented CPOE; 39% have partially implemented Telemedicine; and 7% have fully implemented Telemedicine.

A 2006 survey of HIT adoption in 30 rural or very small hospitals (22% of all Wisconsin hospitals) conducted by the Rural Wisconsin Health Cooperative (RWHC) discovered the following:

- Every hospital has a core Master Patient Index database
- 80% of respondents had installed electronic pharmacy, lab, or order entry systems
- Few hospitals have interface engines, which inhibit information flow inside the hospital and may hinder participation in HIEs.

Wisconsin now has an opportunity to deploy technology to transform health care to achieve a better, safer, and more efficient health care system and thereby improve the overall health of the state's population. Technology provides a platform to manage and access information to transform the health care sector. The Wisconsin *eHealth Action Plan* presented to Governor Doyle on December 1, 2006, lays out a five-year roadmap to achieve this vision. The policy work that is under way with the support of this project sets out the steps to address privacy and security issues that are a barrier to health information exchange.

[4] MetaStar, Inc. Environmental Scan, December 1, 2005 and Simmons G. The prevalence of EHI Technology in Wisconsin, eHealth Care Quality and Patient Safety Board, March 26, 2006.

Section 2 – Assessment of Variation

2.1 Methodology

The Variations Workgroup comprised a wide variety of representative stakeholders including consumers, providers, and state and federal agencies. It included privacy and security experts from 16 different organizations, selected to meet the stakeholder requirements developed by RTI. The Workgroup held four sessions to discuss scenarios developed by RTI to determine current business practices associated with the exchanges of information represented in the scenarios. The Workgroup discussions resulted in:

- Documentation of detailed variations in business practices associated with each scenario,
- Determination of the driver of each business practice, and
- Assessment of business practices that pose barriers to health information exchange (HIE).

The Legal Workgroup comprised stakeholders representing consumers, providers and various state agencies, and included 15 privacy and security 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 drivers of business practices and legal barriers to HIE, and to determine which barriers identified by the Variations Workgroup are driven by law versus business practice or policy.

The Interim Assessment of Variations Report contained the results of the Variations and Legal Workgroups' analyses. A Solutions Workgroup was then assembled to review the barriers to HIE as determined by the Variations and Legal workgroups and develop solutions to the barriers while maintaining privacy and security standards. Finally, an Implementation Workgroup was convened to finalize the solutions and 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 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

2.1.a Variations Workgroup

Membership

Wisconsin's Variations Workgroup was developed to have one representative for each stakeholder group required by the grant. Invitations were sent 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
- Research
- 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

The Department of Health and Family Services (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 read to the group, assumptions were identified, business practices were acknowledged and potential barriers to exchange were highlighted for the group to consider. The Workgroup identified business practices and policies related to the scenarios provided by RTI and determined which practices posed barriers to HIE. Each scenario was evaluated in terms of the nine domains of privacy and security provided by RTI. The project team developed a structured methodology for collecting from Workgroup members the business policies and practices, assumptions, and the driver for the business practice identified. The project team was responsible for recording this information, assigning the domain, and assisting in identification of barriers based on the discussion and the definition provided by RTI.

Following the first meeting, the project 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, Workgroup members were given opportunities to identify 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 of the Variations Workgroup 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 identified business practices was provided for the group to review. This document highlighted where variations in practice, policy, or law were observed.

2.1.b Legal Workgroup

The Legal Workgroup comprised 15 members from the Privacy and Security Workgroup of Wisconsin's HIPAA Collaborative of Wisconsin (COW). This non-profit organization is open to entities considered to be Covered Entities, Business Associates, and/or Trading Partners under HIPAA, as well as any other organization affected by HIPAA regulation.

The members of this Workgroup represented the following stakeholders:

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

The Legal Workgroup 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 Privacy Workgroup, a group that recently completed an analysis of interface between state and federal privacy laws. This expertise enhanced Wisconsin's Security and Privacy Project effort.

The Legal Workgroup held a series of meetings, each of which followed a Variations Workgroup meeting, so the Legal Workgroup could work from the results of the Variations Workgroup. The purpose of the Legal Workgroup was to identify and analyze the legal drivers for the business practices identified by the Variations Workgroup. The Legal Workgroup was charged with analyzing variations in privacy and security 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 Legal 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.

In an effort to simplify the process, the project 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 whether the legal drivers identified presented a barrier to exchange

of health information in both paper and electronic environments. Some Legal Workgroup members have experience with electronic health records, 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 Legal Workgroup's review, the Privacy Consultant reviewed the Workgroup's findings and wrote a summary of the legal analyses.

2.2 Summary of Relevant Findings-Purposes for Information Exchange

2.3 Treatment (Scenarios 1–4)

The Variations and Legal workgroups were given four treatment scenarios to analyze in order to find variations in current business practices, the drivers of the business practices, and barriers to the exchange of health information.

2.3.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to the discussion of the treatment scenarios:

- Clinicians
- Clinics – Large, small
- Consumers or Consumer Organizations
- Federal Health Facilities
- Home Care and Hospice
- Hospitals
- Long Term Care Facilities and Nursing Homes
- Physician Groups
- Professional Associations and Societies
- Payers
- Department of Health and Family Services
- State Mental Health facility

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

2.3.b 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.

The workgroups made the assumption that the information requested did not include mental health information. Inclusion of "sensitive" information would be reviewed in detail in Scenario 2.

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 was deemed necessary varied between Workgroup members. This is interesting in that neither state nor federal law requires the application of the "minimum necessary" restriction for records released for treatment.

Legal Analysis

The legal analysis in this scenario requires a determination of which state and federal privacy laws apply to the inpatient information requested. If the information requested is general health care information, Wisconsin Statutes section 146.81-146.84 and the HIPAA Privacy Rule will apply. If the information requested fits the legal protection afforded mental health, alcohol and other drug abuse and developmentally disabled patient information, then Wisconsin Statutes section 51.30, the HIPAA Privacy Rule and 42 CFR Part 2 may apply.

A written authorization is not required under state or federal law[5] to exchange patient information between providers for treatment purposes unless the inpatient information includes specifically protected information such as for mental illness.[6] 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. Two Wisconsin laws are relevant to this scenario: Wisconsin Statutes section 146.81-146.84[7] and 51.30.[8] Wisconsin Statutes section 146.81-146.82 govern general health care information and contain an exception that allows for release of patient care information from provider to provider for patient treatment without patient consent. This state law is consistent with the Federal Privacy Rule, which also does not require patient consent for disclosure from provider to provider for treatment, and consent would not be required.[9] If the inpatient information requested is general health care information under Wisconsin Statutes section 146.81, then patient consent would not be required.

If the information requested relating to the anti-psychotic drug is from a Wisconsin hospital, is "sensitive" under Wisconsin law (i.e., relating to mental illness, developmental disabilities, or alcohol and other drug abuse) and is protected under Wisconsin Statutes section 51.30, specific, written patient consent is required to authorize the health information exchange.[10] If the request originates in Wisconsin and is directed to an out-of-state facility, then the law of the state in which the information is contained would

[5] Wisconsin Statutes section 146.82(2)(a)2; 45 CFR 164.502(a)(1)(ii) and 164.506(c)(2),
[6] Wisconsin Statutes section 51.30(4)(b)8 and 8g
[7] Wisconsin Statutes section 146.81 – 146.84
[8] Wisconsin Statutes section 51.30
[9] 45 CFR 164.506(c)(2)
[10] Wisconsin Statutes section 51.30

apply. State laws regulating the disclosure of "sensitive" patient information may differ and it may be difficult to determine whether patient consent is required.

If Wisconsin Statutes section 51.30 applies in this scenario and the HIPAA Privacy Rule also applies, Wisconsin law is more stringent and more protective by requiring patient consent for disclosure and Wisconsin law would preempt the Federal Privacy Rule. 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 other drug abuse or developmental disability 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.[11]

The Federal Privacy Rule applies a "minimum necessary" standard to the amount of information disclosed; this law does not require that the standard be applied when the exchange is for treatment. However, Wisconsin Statutes section 51.30 and HFS 92.03(1)(n), Wis. Admin. Code, also contain a "minimum necessary" standard that does apply to an exchange for treatment. So, if s.51.30 applies, the more stringent state law would again preempt HIPAA and the "minimum necessary" law would apply.

Legal Barriers

Federal law requires that the identity of the requester be verified.[12] State law does not have a specific provision requiring verification of the requester. In this scenario, most of the stakeholders would have verified the identity of the requester. This requirement for a verification process presents a barrier to health information exchange.

Although HIPAA would not require documentation of disclosures for treatment[13] as depicted in this scenario, Wisconsin Statutes section 146.82(2)(d) requires documentation of disclosures made by a health care provider when made without the consent of the patient. Wisconsin Statutes section 51.30, if applicable, also requires documentation of disclosures for treatment. This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, the following requirements would need to be met and will present barriers to the exchange of information.

- Method of exchange and security measures for protection of exchange[14]
- Requirements for receipt of the information[15]

[11] Wisconsin Statutes section 51.30 (2)
[12] 45 CFR 164.312(d); 45 Cfr 164.514(h)
[13] 45 CFR 164.528(a)(1)(i)
[14] Security and Privacy Rules
[15] Wisconsin Statutes section 146.82; 45 CFR 164.501 Definition of designated record set

In addition, HIPAA allows a patient to request that restrictions be imposed on the information exchanged and the provider must review and respond to that request.[16] This right of restriction may cause additional barriers to information exchange.

This scenario described 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; and variability in state laws may present a barrier to health information exchange.

Scenario 2 – Patient Care Scenario B

An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The two organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol 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, a request from the primary care provider for information from the substance abuse facility, would be protected more stringently under Wisconsin law than federal law, and consent for disclosure between providers for treatment would be required. Some Variations Workgroup members responded that they would require consent, while some would provide 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 of the substance abuse information, prohibited by state law without patient consent, met with varied responses. One responder had a policy that incorporated the substance abuse information into its facility's record when received, arguably allowing it to re-disclose the substance abuse information as the facility's record and not as a re-disclosure. Other Workgroup members would re-disclose the information (obtained from the treatment facility) to the specialist without consent. Others would require consent to re-disclose information. Again, this shows the variability in interpreting 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 by mail, some by fax.

Legal Analysis

The Federal Privacy Rule allows disclosure of patient information from provider to provider for treatment purposes without patient consent. However, Wisconsin privacy law and the federal law regulating alcohol and other drug treatment records impose more stringent standards and require patient consent for

[16] 45 CFR 164.532(a)

sensitive patient information such as mental health, alcohol and other drug abuse, and developmental disability information.[17]

The Federal Privacy Rule requires scrutiny of the amount of patient information disclosed. It does not require application of the "minimum necessary" standard for records released for treatment, but Wisconsin law[18] does apply this standard for more sensitive patient information (alcohol and other drug abuse).

The Federal Privacy Rule does not require that disclosures for treatment be documented, but again a more stringent standard applies under Wisconsin law and documentation is required.[19]

Legal Barriers

Wisconsin statutes, dating from 1977, regulate and stringently protect patient information relating to mental health, alcohol and other drug abuse, and developmental disability. Wisconsin law and the federal law regulating alcohol and other drug abuse patient information require patient consent authorizing information exchange between providers for treatment purposes.[20] The Federal Privacy Rule allows disclosure without patient consent, and this divergence in state and federal laws requires interface between state and federal law that is specifically addressed under HIPAA.[21] The resolution, by federal law, is to apply the law (state or federal) that provides the most protection for the patient information. In this scenario, HIPAA would require application of the more stringent requirements under state and federal law; consent from the patient would be required for disclosure of the substance abuse facility information to the primary care provider.

In addition, state[22] and federal[23] 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 require patient consent.

The Workgroup determined that anytime consent is required to exchange information it creates a barrier to exchange. The process to share information requires a determination of whether consent is required this analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

The Federal Privacy and Security Rules require that the identity of a requester for protected health information be verified to determine that individuals are who they claim to be. In this scenario, verification of the primary care provider requesting the patient information would be required. This requirement presents a barrier to health information exchange.

Although HIPAA would not require documentation of disclosures for treatment,[24] Wisconsin Statutes section 146.82(2)(d) and 51.30 require documentation of disclosures made by a health care provider. This

[17] 42 CFR Part 2; Wisconsin Statutes section 51.30
[18] HFS 92.03(1)(n), Wis. Admin. Code
[19] Wisconsin Statutes section 51.30(4)(e)
[20] Wisconsin Statutes section 51.30(2); 42 CFR 2.1
[21] 45 CFR 160.203(b)
[22] HFS 92.03(1)(h) , Wis. Admin. Code
[23] 42 CFR 2.31

documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

The Federal Privacy Rule requires scrutiny of the amount of patient information disclosed, but does not require application of the "minimum necessary" standard for information released for treatment, however Wisconsin law does apply this standard in this scenario for more sensitive patient information.[25]

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, the following requirements would need to be met and will present barriers to the exchange of information.

- Method of exchange and security measures for protection of exchange[26]
- Requirements for receipt of the information[27]

Scenario 3 – Patient Care Scenario C

At 5:30 pm 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.

[24] 45 CFR 164.528(a)(1)(i)
[25] HFS 92.03(1)(n) , Wis. Admin. Code
[26] Federal Security and Privacy Rules
[27] Wisconsin Statutes section 51.30; 45 CFR 164.501 Definition of designated record set

Variations Workgroup Summary

The Variations Workgroup members described a variety of practices for sending sensitive information from an inpatient psychiatric unit to a skilled nursing facility, when a patient is being transferred between facilities, including whether they would require patient consent. Wisconsin law requires patient consent for this disclosure, so practice demonstrates variation in interpretation and application of Wisconsin privacy requirements for more stringently protected patient information.

All Workgroup members would exchange information without patient consent between a physician and his/her transcription service because a written business agreement exists. This agreement may be an employment contract or a business associate contract.

All Workgroup members would exchange patient information between 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 other drug abuse or developmentally disabled information, even though Wisconsin law requires patient consent.

The work group members reported a variety of practices for disclosure processes for information related to an inpatient psychiatric stay, verification of requester, methods for information exchange, policies for auditing/documenting disclosures and 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 in 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 law.[28] 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, patient consent for exchange would be required by Wisconsin law and possibly the federal law regulating alcohol and other drug abuse records.[29] In addition, Wisconsin law requires that patient information be sent with the patient when transferring from an inpatient facility to a nursing home facility.[30] So the patient records would be required to be sent to the nursing home facility with patient consent.

All stakeholders agreed patient information could be shared between the physician and his transcription company without patient consent, but that some type of contractual relationship such as employment or a business associate agreement would be required to allow this exchange.

[28] Wisconsin Statutes section 146.82(2) (a) 2. a and b; 45 CFR 164.506(c)(2);
[29] Wisconsin Statutes section 51.30(2); 42 CFR 2.1
[30] HFS 132, Nursing Home Records, Wis. Admin. Code

The stakeholders generally agreed that they would not require patient consent for disclosure of the physician's transcription to the nursing home as this appears to be a provider-to-provider information exchange of non-sensitive information for treatment and there appears to be a relationship between the physician and the nursing home. If the physician's dictation is regulated by 51.30, because it contains sensitive health care information, consent would be required to share between non-related-entity providers.[31]

Legal Barriers

Consent
In this scenario, if the information exchanged were mental health, alcohol or other drug abuse, or developmental disability information, the exchange between providers for treatment purposes would require patient consent.[32] This would include the exchange between the hospital inpatient psychiatric unit and the nursing home, and the nursing home and the psychiatrist.[33]

For information to be exchanged between a physician and a transcription employee or company, the Federal Privacy Rule would require some type of contractual relationship such as employment or a business associate agreement. The Federal Privacy Rule requires that the agreement between the physician and the transcription company be in writing and meet specific requirements before exchange can occur.[34] Wisconsin law does not control this exchange as it is considered a use, not a disclosure. In this case, federal law is more stringent than state law and presents a barrier to health information exchange.

Minimum Necessary
The Federal Privacy Rule requires scrutiny of the amount of patient information disclosed, but does not require application of the "minimum necessary" standard for information released for treatment. However, Wisconsin law does apply this standard in this scenario for more sensitive patient information.

If information is transferred electronically, there is no controlling Wisconsin law relating to transmission security but the Federal Security Rule, when applicable, would require that the transmission be secure.[35] Wisconsin law also requires that disclosure of the patient health record from the inpatient psychiatric unit be documented.[36] The Workgroup determined that both the requirements for a secured transmission and documentation of the disclosure present barriers to information exchange.

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.

[31] Wisconsin Statutes section 51.30 (2)
[32] Wisconsin Statutes section 51.30(2); 42 CFR 2.1
[33] Wisconsin Statutes section 51.30 (2)
[34] 45 CFR 164.502(e)(1)
[35] 45 CFR 164 Subpart C
[36] Wisconsin Statutes section 51.30(4)(e)

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 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

Patient consent is not required to disclose a patient's record containing an HIV test result, from provider to provider for treatment, under either state or federal law.[37] Therefore, the information exchange between the patient's providers would not require patient consent. The Federal Privacy Rule would also not require that this disclosure for treatment purposes, or the disclosure authorized by consent to the niece, be documented or that the "minimum necessary" standard apply.

Legal Barriers

The Legal Workgroup agreed, consistent with state and federal law, that the disclosure of the aunt's genetic information from a provider to the niece would require 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 valid patient consent with the appropriate legally authorized signature for a deceased patient's information was identified as a barrier to health information exchange.[38]

Wisconsin law would require that the disclosure between providers and the disclosure to the niece be documented under Wisconsin Statutes section 146.82(2)(d) and maintained as a part of the patient's health care record. The stringency of the documentation requirement presents a barrier to health information exchange.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, then the following requirements would need to be met and would present barriers to the exchange of information.

- Method of exchange and security measures for protection of exchange[39]
- Requirements for receipt of the information[40]

[37] Wisconsin Statutes section 252.15(5)(2); Wisconsin Statutes section 146.82(2)(a)2.; 45 CFR 164.502(a)(1)(ii) and 164.506(c)(2),
[38] Wisconsin Statutes section 146.81(2) and (5); 45 CFR 165.508
[39] Security and Privacy Rules

2.3.c 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 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.

2 - Information authorization and access controls

The treatment scenarios highlighted several discrepancies in information authorization and access controls among the stakeholders. Some variation is due to the fact that very few of the stakeholders use electronic medical records systems. Those who do have varying levels of controls, and those who do not have the means to control access to health information.

One of the representative organizations has an electronic medical records system 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 records system 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.

[40] Wisconsin Statutes section 146.82 and 252.15; 45 CFR 164.501 Definition of designated record set

Facilities with paper records have no way to limit access to their records and cannot audit who has viewed which records. One of the stakeholders with both paper and electronic records systems 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 about whether a non-network provider would have access to the facility's records. Some of the stakeholders stated that the provider would need a contractual arrangement to access the facility's records, while others stated that access would be allowed with or without consent as provider to provider. Similarly, most stakeholders would not 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 each 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 barriers to health information exchange, but they may be necessary barriers to provide privacy and security to patient health care 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 the stakeholders have policies to ensure that the correct patient information is included when 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, consent is used to verify the identity of the patient and the request form is used to verify the identity 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 the facilities match the signature on the consent with the patient's signature on file before releasing information. For organizations who also verify the provider, the medical license number and provider signature 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 is a barrier 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 the way requests for patient information are made. Some send written requests for patient information in the mail while others send requests via fax. If the physician has a relationship with the facility that has the record, 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 records system. 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 processes 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)

Those stakeholders with electronic medical records systems can 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 is authorized to modify patient records. The small physician practice queried did not have policies stating who was allowed to modify records; instead they use “good practice” to determine who may edit patient records. Variability in practice related to authorization for modification and protection of data integrity may create barriers to 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, the stakeholders varied as to whether or not they logged the release. Typically if medical records clerks release the information, they log the requester 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 records system, often the technology itself logs the disclosure by capturing who accessed the information. Despite the state policies, all said that not every disclosure is documented, in practice, especially when physicians disclose the information.

The organizations without electronic health records systems do not have processes 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 the organizations always monitor access to "very important persons" records.

The statutory requirements for documentation of disclosures, specifically those 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 Workgroup member who is a clinician in a small practice does not need any identification to enter his building; however, other organizations in the Workgroup require 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 the department to which 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 enforced 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 law is more stringent than federal law, and this creates a barrier to health information exchange. Barriers are also caused when the law is not clear, and when interpretations of the law vary in practice.

Consent
Wisconsin law requires patient consent to release sensitive, more stringently protected, patient information, which includes mental illness, substance abuse or developmental disability information. Wisconsin law does not require consent to release HIV test results from one provider to another for treatment purposes; however, many of the stakeholders would require consent to release this information. Wisconsin 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 law requires several elements to the consent which vary from federal law. In general, most patient consent forms 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 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 this 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 the stakeholders discussed for disclosure of information were governed by policies; many of these 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 these policies follows.

1. Obtain a declaration from the facility for the out-of-state facility that this is an emergency.
    - The requester must declare the purpose of request as a medical emergency. If request is verbal, requester 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 requester of patient information.
    - All stakeholders have verification processes, but the policies vary.
    - Some verify requester 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 patient consent to release sensitive information.
    - Scenario 3: Some of the 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 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 according to 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 this 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.

2.3.d Critical Observations

Unique to Wisconsin

The treatment scenarios highlight two major barriers to health information exchange that are created by Wisconsin law. The first is the requirement for patient consent to exchange sensitive information for treatment purposes (mental health, alcohol and other drug abuse, developmental disability information) that is more stringent than federal law, which does not require consent under these circumstances.

The second barrier, unique to Wisconsin, is caused by the laws governing the documentation of disclosures of health care information. Legal requirements for documentation of disclosures make the exchange of health care information more difficult. The 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 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.

Consent is 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 law, resulting in barriers to exchange across state lines. In addition, while consent for disclosure of HIV test results is not required by law, most stakeholders have policies requiring consent in

such cases, even for treatment purposes. The consent requirement is driven by both law and policy and poses barriers to information exchange.

Documentation of disclosures
Wisconsin regulations requiring the documentation of disclosures pose significant barriers to exchange. These requirements are rigorous and difficult to interpret; consequently, there are variations in how the documentation is completed. 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 the "minimum necessary" increase the amount of time required to exchange health information. In the Workgroup's experience, often technology cannot limit disclosures to the "minimum necessary," so processes that could be electronic need to be handled manually. For organizations that use paper records, sifting through records to make sure that only 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, whether by phone, in writing, or by fax, when linked with specific requirements for the format of requests, creates barriers to efficient exchange of patient information.

2.4 Payment (Scenario 5)

2.4.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to the discussion of the payment scenario:

- Clinicians
- Consumers
- Federal Health Facilities
- Hospices
- Hospitals
- Long Term Care
- Payers

- Physician Groups
- Associations
- State Agencies

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

2.4.b 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 health care 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 health care 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 in which organizations have invested 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 Workgroup members 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 accessed. 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 purposes.[41] None of the stakeholders were comfortable with the concept of allowing the payer unlimited access to patient information. If the payer requested full access to the EHR, including patient information not necessary to determine

[41] Wisconsin Statutes section 146.82(2)(a)3; 45 CFR 164.502(a)(1)(ii) and 164.506(c)(3)

payment, patient consent is required. If the payer requested information related to an HIV test result, mental health, alcohol and other drug abuse, or developmental disability, consent would be required.[42]

Legal Barriers

Verification of the payer making the request for the pre-authorization information would be required by federal law.[43] This requirement presents a barrier to health information exchange.

Documentation of the disclosure for payment purposes, although not required by federal law, would be required by state law.[44] This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Although there is no applicable state limitation, federal law requires that the information disclosed for payment purposes be limited to that which is "minimally necessary" to be able to make payment for the service provided.[45] The application of this standard presents a significant barrier to health information exchange.

An additional barrier to health information exchange identified in this scenario relates to security of information transfer and transmission. The HIPAA Security Rule applies to the electronic exchange of health care information and would require that the exchange in this scenario meet the Security Rule requirements for a secured transmission, which presents a barrier to the exchange of information.

2.4.c Domains

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

1 - User and entity authentication
2 - Information authorization and access controls
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 require either a written agreement or a business associate agreement between the health care provider and the payer. Many of the stakeholders would not grant access to a payer to any part of their health records.

[42] Wisconsin Statutes section 252.15; Wisconsin Statutes section 51.30; 45 CFR 164.512
[43] 45 CFR 164.514(h)
[44] Wisconsin Statutes section 146.82(2)(d); 51.30(4)(e)
[45] 45 CFR 164.502(b)(1)

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

One organization in the Workgroup allows a payer access to their electronic medical records system. 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 systems 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 the "minimum necessary" standard. A majority of the 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.

4 - Information transmission security or exchange protocols

In most cases, access was not granted because systems cannot control to whom or 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 Wisconsin Administrative Code.

8 – State law restrictions

Consent
Wisconsin 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 disability) information for payment purposes. For access to a complete health record, consent is required by state law.

Minimum Necessary
Federal and Wisconsin law allow access only to the "minimum necessary" information to achieve the purpose for the disclosure. However, with the exception of one hospital, current technology does not allow limiting access to the "minimum necessary," so this law creates a barrier to exchange.

Documentation of Disclosure
Wisconsin 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 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 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, the stakeholders would not release this information outside a system network. This is due to 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.

2.4.d Critical Observations

Unique to Wisconsin
The payment scenario highlights three barriers to health information exchange that are unique to Wisconsin. First, Wisconsin law mandates verification of the requester 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 constitutes 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 record contains 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 systems who stated they would not allow a payer to access their health records said 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, some Workgroup members believe that current technology cannot specify the type of access that is granted. For them, 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 requester. 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 systems 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
As above, because some Workgroup members believe technology cannot currently limit access to records or to a specific portion of the record, they saw no way to exchange information in this way without violating the "minimum necessary" requirements.

2.5 RHIO (Scenario 6)

2.5.a Stakeholders

Although the Variations and Legal workgroups included all the stakeholder representation required by RTI, the current state of RHIO development in Wisconsin did not provide for representation from an active and currently operational RHIO. The stakeholders represented, however, had discussed and investigated the formation of RHIO relationships. Those stakeholders are listed below:

- Clinicians
- Hospitals
- Payers
- Physician Groups

2.5.b Summary of Findings

This section contains the scenario followed by findings from the Variations and Legal workgroups relevant to the formative stages of RHIOs in Wisconsin.

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

Variations Workgroup Summary

The relevant Workgroup stakeholders have not yet formed RHIOs. The exploratory steps taken have, however, led them to agree that under state and federal privacy laws, sharing of patient identifiable data between participating organizations would not be allowed without a business associate agreement meeting the HIPAA Rule requirements, an inter-facility relationship, a legal contractual arrangement or statutory exceptions allowing access without the patient's informed consent for disclosure.

Legal Analysis

According to state and federal law, sharing of patient identifiable data between participating organizations would not be allowed without a business associate agreement meeting the HIPAA Rule requirements, an inter-facility relationship, a legal contractual arrangement or statutory exceptions allowing access without the patient's informed consent for disclosure.

Legal Barriers

Verification of the requester for the identifiable information would be required by federal law.[46] This requirement presents a barrier to health information exchange.

Sharing of patient identifiable data between participating organizations would not be allowed without a business associate agreement meeting the HIPAA Rule requirements, an inter-facility relationship, a legal contractual arrangement or statutory exceptions allowing access without the patient's informed consent for disclosure. These requirements present significant barriers to health information exchange.

Although there is no applicable state limitation, federal law requires that the information disclosed be limited to that which is "minimally necessary."[47] The application of this standard presents a significant barrier to health information exchange.

An additional barrier to health information exchange identified in this scenario relates to security of information transfer and transmission. The HIPAA Security Rule applies to the electronic exchange of health care information and would require that the exchange in this scenario meet the Security Rule requirements for a secured transmission, which will present a barrier to the exchange of information.

2.5.c Domains

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

1 - User and entity authentication
2 - Information authorization and access controls
4 - Information transmission security or exchange protocols
8 - State law restrictions
9 - Information use and disclosure policy

1 – User and entity authentication

The stakeholder responses provided were all related to discussions anticipating a RHIO agreement rather than based on participation in an active RHIO relationship. For those Workgroup members who represented organizations that would share their electronic health information within a RHIO arrangement, they would either require a written agreement or a business associate agreement between the participants.

In order to access the shared system, the stakeholders expected that users would be required to login with a user name and password.

[46] 45 CFR 164.514(h)
[47] 45 CFR 164.502(b)(1)

2 - Information authorization and access controls

In order to access the shared system of the planned RHIO relationship, the stakeholders expected that users would be required to login with a user name and password.

4 - Information transmission security or exchange protocols

Stakeholders expect that information transmission security as required under HIPAA would be a required part of the RHIO system.

8 – State law restrictions

According to state law, sharing of patient identifiable data between participating organizations would not be allowed without a business associate agreement meeting the HIPAA Privacy Rule requirements, an inter-facility relationship, a legal contractual arrangement or statutory exceptions allowing access without the patient's informed consent for disclosure.

Confidentiality

Wisconsin law requires that all information accessed be maintained as confidential. This is a barrier to exchange because information obtained has to be handled carefully so that patient confidentiality is maintained.

9 - Information use and disclosure policy

Sharing of patient identifiable data between participating organizations would not be allowed without a business associate agreement meeting the HIPAA Privacy Rule requirements, an inter-facility relationship, a legal contractual arrangement or statutory exceptions allowing access without the patient's informed consent for disclosure.

2.5.d. 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).[48] WHIE has established a formal governance and membership structure, but has not yet entered into the implementation stage or begun to exchange data.

WHIE was awarded an eHealth Initiative contract worth $110,000 from the State of Wisconsin for calendar year 2006. The funds allow WHIE, created in 2005 as a not-for-profit 501c3 entity, to develop its governance structure and administrative staff. To monitor the beginnings of potentially significant community health events through sharp increases in emergency room traffic, the contract also will enable WHIE to develop a plan for a pilot regional patient encounter index linked to a state surveillance system.

[48] 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).

Dr. Ed Barthell, a co-founder of WHIE, said the organization's initial pilot projects will be aimed at providing emergency clinicians with software tools that lead to improved quality and efficiency of emergency care provided to Medicaid patients.

Other projects identified by WHIE include the creation of a regional medication reconciliation system that serves all patients, and the implementation of an electronic results routing and messaging system to improve efficiencies in multiple outpatient clinics. According to the organization, these latter projects will not be undertaken until more funding is obtained.

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 was submitted to the Governor in December 2006, which will serve as a catalyst for the development and implementation of RHIOs in Wisconsin. The issues related to data 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.

Major Barriers to Exchange

Sharing of patient identifiable data between participating organizations would not be allowed without a business associate agreement meeting the HIPAA Privacy Rule requirements, an inter-facility relationship, a legal contractual arrangement or statutory exceptions allowing access without the patient's informed consent for disclosure.

2.6 Research (Scenario 7)

2.6.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to 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.

2.6.b 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 Institutional Review Board (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 six-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, the waiver was obtained through this process 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 consent[49] for research purposes are less stringent than HIPAA[50] and federal law would control. Therefore, consent would not be required for disclosures related to the IRB-approved research project.

Legal Barriers

In this scenario, both requests for disclosure of patient information appear to be outside IRB approval and 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. Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

[49] Wisconsin Statutes section 146.81(2)(a)6, 51.30(4)(b)3, 252.15(5)(a)10
[50] 45 CFR 164.512(i)

If HIPAA applies to the research project then the following statutory requirements would present barriers to health information exchange:

- Verification of the requester
- Application of the "minimum necessary" standard
- Security in the electronic transfer of information
- Documentation of disclosures.

2.6.c 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 so that researchers only have access to the research data.

3 – Patient and Provider Identification

Some of the 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

Methods of how the researcher receives patient data vary across the 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 the stakeholders discussed relating to these research scenarios were governed by policies; many of these policies are in place to ensure compliance with state and federal laws. A summary of the policies follows:

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 six 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 six months without additional consent, even with a written policy that all changes go to the IRB for approval.

3. Researcher 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 additional consent, even with a written policy that all changes go to the IRB for approval.

2.6.d Critical Observations

Unique to Wisconsin

There is nothing unique to Wisconsin laws that affect 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.

2.7 Law Enforcement (Scenario 8)

2.7.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to the discussion of the law enforcement scenario:

- Clinicians
- Consumer
- Hospitals
- Other (Large Clinics)
- Other (Small clinics)
- Physician Groups
- Correctional Facilities
- Federal Health Facilities
- Laboratories
- State Government
- Community Clinics and Health Centers

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

2.7.b 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 oral), as was the method of disclosure.

Legal Analysis

Under the scenario it was not clear if the blood draw was performed for treatment purposes or at the request of law enforcement for the determination of intoxication related to the automobile accident. 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 from access by law enforcement under Wisconsin law and the result would have been accessible to law enforcement.[51] No barrier would have been presented to this exchange of information.

Legal Barriers

If the blood draw in this scenario 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.[52] Because the patient is of the age of majority in Wisconsin, consent would be required to release patient information to the parents.[53] Any time consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

HIPAA would require that the identity of the individuals requesting the patient information, in this case law enforcement and the parents, be verified.[54] This requirement presents a barrier to health information exchange.

Although federal law would not require documentation of a disclosure with patient consent, documentation is required under Wisconsin Statutes section 146.82(2)(d). This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the following requirements would need to be met and will present barriers to the exchange of information:

- Determination of information to be disclosed and application of "minimum necessary" standard[55]
- Method of exchange and security measures for protection of exchange[56]

2.7.c Domains

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

1 - User and entity authentication

[51] Wisconsin Statutes section 146.81(4)
[52] Wisconsin Statutes section 146.82(1)
[53] Wisconsin Statutes section 146.82(1), 146.81(5)
[54] 45 CFR 514(h)(1)
[55] 45 CFR 164.502(b) "minimum necessary"
[56] Security and Privacy Rules

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 requester 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 varies across the 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.

4 - Information transmission security or exchange protocols

Representative organizations vary in how they disclose information to law enforcement. Some orally 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 no 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 discloses the information orally to the parents, even if consent was obtained, most agreed that the disclosure is rarely documented in practice.

8 – State law restrictions

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

Documentation of Disclosure
Wisconsin 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 oral release of information to parents.

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

Minimum Necessary
The information released is limited to the "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 require a faxed request on letterhead.
    - In practice, some don't require a formal request if a uniformed law enforcement officer is in the ER.

2.7.d Critical Observations

Unique to Wisconsin

Wisconsin law mandates documentation of disclosure of health information. Every disclosure must be documented, and 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 for sensitive information is more restrictive than HIPAA.

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 oral 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 cumbersome with current technology for electronic exchange.

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

2.8.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to 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.

2.8.b 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 patient consent.

Stakeholders varied 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 from the patient, 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 a health plan[57] 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.[58]

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

[57] 45CFR 164.103
[58] 45 CFR 164.502(2)(e); 45 CFR 164.504(e); 45 CFR 164.506(c)(3)

purposes.[59] If the Geodon prescription is considered to be sensitive patient information and is regulated by Wisconsin Statutes section 51.30, consent would be required for disclosure for payment purposes from the physician to the PBM.

Legal Barriers

If the self-insured hospital is considered to be a covered entity[60] under HIPAA, a business associate agreement would be required to enable the self-insured hospital to share information with the PBM.[61] The legal requirements and the process required to obtain a business associate agreement present a barrier to health information exchange.

If the Geodon prescription is considered to be mental health information, the controlling law would be Wisconsin Statutes section 51.30 and more stringent protections would apply. 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 purposes under this Wisconsin law.[62] The Workgroup members felt that any time consent is required to exchange information it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

The federal Privacy and Security Rules require that the identity of a requester for protected health information be verified to determine that individuals are who they claim to be. In this scenario, verification of the PBM requesting the patient information would be required.[63] There is no similar requirement in Wisconsin law unless the Geodon is mental health information and then verification of the requester is also required under Wisconsin law.[64] This requirement presents a barrier to health information exchange.

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.[65] If the disclosure is for payment purposes, HIPAA and state law would require application of the "minimum necessary" standard.

Documentation of the disclosure of general health information or sensitive health information, although not required by federal law, would be required by state law and under the preemption analysis, state law would control.[66] This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

[59] Wisconsin Statutes section 146.82(2)(a)2; 45 CFR 164.506(c)2
[60] 45 CFR 164.103
[61] 45 CFR 164.502(2)(e); 45 CFR 164.504(e); 45 CFR 164.506(c)(3)
[62] Wisconsin Statutes section 51.30(4)
[63] 45 CFR 164.514(h)
[64] HFS 92.03(1)(m), Wis. Admin. Code
[65] HFS 92.03(n) , Wis. Admin. Code
[66] Wisconsin Statutes section 51.30(4)(e)

If the exchange is electronic, HIPAA would require that the prescribing physician secure the transmission to the PBM.[67]

Scenario 10 – Pharmacy Benefit Scenario B

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

Variations Workgroup Summary

The Workgroup agreed that a business agreement between Company A and the PBMs 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.[68]

Legal Barriers

Whenever a business associate agreement (BAA) is required there are barriers to information exchange. The BAA must contain required statutory elements and must often be reviewed and approved by legal counsel. This agreement, which may be necessary to assure patient confidentiality, would present a barrier to health information exchange.

Under federal law, PBM2, as the business associate of company A, would be required to verify the identity of the requester PBM1.[69] This requirement presents a barrier to health information exchange.

Disclosures within this scenario would be controlled by the HIPAA "minimum necessary" standard[70] and the application of this standard presents a barrier to health information exchange.

If the sharing of information is electronic, under the HIPAA Security Rule the exchange would be required to be secured.[71]

[67] 45 CFR 164 Subpart C
[68] 45 CFR 164.504(e)(1)
[69] 45 CFR 164.514(h)
[70] 45 CFR 164.514(d)
[71] 45 CFR 164 Subpart C

2.8.c 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 of the two scenarios has a party requesting the information whose identity 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 the form of a contract. Relevant identifying information for both parties would be included 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 the 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 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 returns the requested information using the same means by which the request was made.

The 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 to a PBM's data

would typically not occur. Instead, access would be given by CD or other transportable medium 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 law requires 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 patient 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 fully-insured plans are. Wisconsin state regulations that govern exchanges between fully-insured companies do not apply to Company A.

Business Agreement

In Scenario 10, Wisconsin 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 this exchange would require such an 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. (45 CFR 164.504(e)(1) 2, 45 CFR 164.501)

2.8.d Critical Observations

Unique to Wisconsin

In Scenario 9, Wisconsin 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 patient consent, which presents a barrier to exchange. Furthermore, the consent must meet statutory requirements for a valid consent under Wisconsin law, which serves as a barrier because the elements may differ from required elements in other states.

Wisconsin law also requires documentation of disclosure (Wisconsin Statutes section 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 law does not regulate this exchange because the exchange would be considered a use of information, not a 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 the exchange of information.

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.

2.9 Healthcare Operations/Marketing (Scenarios 11 and 12)

2.9.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to 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.

2.9.b 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 protected health information (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 an organized health care arrangement or an affiliated network.

In Scenario 11, if ABC Health Care is considered an organized health care arrangement or an affiliated health care arrangement, 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 the six-sigma team appears to meet the definition of health care activities.[72]

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 patient consent for marketing activities.[73] The requirement of patient consent for marketing activities does not apply if the activity does not meet the HIPAA definition of marketing.[74] 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, and patient consent would not be required.

Neither state nor federal law requires documentation of an internal use/disclosure for marketing.

Legal Barriers

State law does not require verification of a requester of identifiable patient information; however, federal law does. This means that all covered entities must have written policies and procedures for verifying and authenticating the identity of a requester of patient identifiable information.[75] Most responses from stakeholders indicated that knowing the requester for an internal exchange would be sufficient verification of identity. This requirement may present a barrier to information exchange.

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. The application of this standard presents a barrier to health information exchange.

[72] Wisconsin Statutes section 146.82 (1); 45 CFR 164.501 Definitions; 45 CFR 164.506
[73] 45 CFR 164.508(a)(3)
[74] 45 CFR 164.501 Definitions - Marketing
[75] 45 CFR 164.514(h)(1)

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.[76] This requirement, if deemed necessary, would be an impediment to the exchange of health care information.

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.

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. Therefore, patient consent would not be required for an internal use. In the event that the 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

[76] Federal Security and Privacy Rules (HIPAA).

internal use of patient information for marketing activities. HIPAA requires patient consent for marketing activities.[77] The way in which HIPAA control over marketing activities may not apply is to determine that the specific activity does not meet the HIPAA definition of marketing and therefore is not controlled by HIPAA.[78]

Based on the HIPAA exclusions from the marketing definition, the following communications under Scenario 12 would be excluded from HIPAA marketing control and patient consent would not be required:

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

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.[79]

Legal Barriers

State law does not require verification of a requester 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 requester of patient identifiable information.[80] Most responses from stakeholders indicated that knowing the requester would be sufficient verification of identity. This process may present a minimal barrier to information exchange.

Generally, marketing activities would be considered an internal "use" and would not be controlled by state law. Therefore, patient consent would not be required for an internal use. In the event that the 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.

The two marketing activities which meet the HIPAA definition of marketing, and therefore require patient consent under HIPAA for this use/disclosure, are the disclosures for fundraising and for marketing with the diaper company. Since the exchange with the diaper company would be deemed a disclosure under Wisconsin law and there is no statutory exception for this type of disclosure, the exchange with the diaper company would also require patient consent under Wisconsin law. Some of the Workgroup members felt that any time consent is required to exchange information it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent. In addition, under HIPAA, when an activity is deemed marketing, the patient must be offered the opportunity to "opt out." The activation of the patient "opt out" would impede information exchange.

[77] 45 CFR 164.508(a)(3)
[78] 45 CFR 164.501 Definitions - Marketing
[79] Wisconsin Statutes section 146.82(d); 45 CFR 164.528
[80] 45 CFR 164.514(h)(1)

Federal law requires that the "minimum necessary" standard be applied to disclosures of identifiable information to an internal marketing department. Most of the stakeholders apply this standard when disclosing information to the marketing department and agree that the application of this standard presents a barrier to health information exchange.

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.[81] This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

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.[82] This requirement, if deemed necessary, would be an impediment to the exchange of health care information.

2.9.c 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

The exchanges of information in these scenarios are internal. Verification processes for internal staff making requests for non-sensitive patient identifiable records vary among the stakeholder organizations. Some would simply verify the requester by the fact that they know them personally. If the request were 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 to which the requesting party has access.

[81] Wisconsin Statutes section 146.82(d); 45 CFR 164.528
[82] Federal Security and Privacy Rules (HIPAA)

3 – Patient and provider identification

In order to process the request, all stakeholders had a process for ensuring the appropriate patients' information is 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

The 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.

Similarly, 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

In all cases, internal disclosures of information for marketing purposes 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 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 purposes as it is deemed health care 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.

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 driven mainly 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 the 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 on a computer network for exchange.

4. Specific information disclosed upon receipt of internal departmental request for identifying patient information.
    - All the stakeholders limit the amount of information disclosed to the "minimum necessary" to meet the needs of the requester.

2.9.d Critical Observations

Unique to Wisconsin

Wisconsin 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, patient consent would be required for the disclosure to the diaper company. The requirement for 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 requester 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
Differing interpretation of legal requirements for consent 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.

2.10 Public Health/Bioterrorism (Scenario 13)

2.10.a Stakeholders

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

- Clinicians
- Physician Groups
- Federal Health Facilities
- Hospitals
- Teaching Hospitals with Research
- Laboratory
- Public Health Agencies
- State Agencies
- Professional Associations
- Consumers or Consumer Organizations

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

2.10.b 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 allows release of patient information without consent. Although state and federal law allow exchange without consent, the Governor also has the power to issue a "state of emergency" declaration 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 an acute infectious disease that can also occur in humans when they are exposed to infected animals or tissue from infected 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.

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

- 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)
- Other law enforcement entities charged with protecting the health of the public

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 type and quantity of information provided would be made on a case-by-case basis.

Legal Analysis

State and federal laws either mandate or allow disclosure of a positive lab test for anthrax without 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.[83] Anthrax is a Category 1 communicable disease, which means notification must occur within 24 hours to the local health officer.[84] According to Wisconsin Statutes section 252.03(2), local health officers may do what is reasonable and necessary for the prevention and suppression of disease. Under the authority of Wisconsin Statutes section 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 given broad authority and emergency management powers under Wisconsin Statutes chapter 252, whereby DHFS may authorize and implement all emergency measures to control communicable diseases, including anthrax. According to Wisconsin Statutes section 252.02(6), DHFS 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 has died, and shall immediately report this occurrence to the local health officer. The local public health officer shall report this information to DHFS.[85] The powers defined in this statute allow the removal of barriers to allow rapid and effective responses to an anthrax threat. Local public health officers are provided with powers similar to those of DHFS; however, they need to keep DHFS updated on measures taken. In addition, Wisconsin is part of an informal group of states

[83] HFS 145.04(2) (d), Wis. Admin. Code
[84] HFS 145 Appendix A; Wisconsin Statutes section 252.05(5)
[85] HFS 145.04(2)(d), Wis. Admin. Code

(Greater Board of Health Initiative) which will share data interstate in the event of communicable disease outbreaks.

State law allows the Governor to declare an emergency, and that order empowers the exchange of information relating to, in this case, a communicable disease.[86]

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, U.S. mail, etc., to all health care 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, it may contain other elements of protected health information such as demographic characteristics, age, gender, etc. However, if identifying the patient is necessary to help find cases of anthrax, then the patient's identity would probably be disclosed. Wisconsin law will allow this, and the decision would be based on balancing a patient's privacy versus protecting the public. In Wisconsin there are no privacy barriers to prevent exchanging this information.[87]

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.[88]

Neither state nor federal law presents privacy barriers, such as requiring patient consent, for the disclosures within this scenario.

This scenario did not present an information exchange in which there is a request for information, so the requirement for verification of the requester did not need to be met in this scenario and did not present a barrier to information exchange.

Legal Barriers

State and federal law require the documentation of disclosures within this scenario, although the stakeholder practices were variable.[89] This requirement presents barriers in health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, the following requirements would need to be met and will present barriers to the exchange of information:

- Determination of information to be disclosed[90]
- Method of exchange and security measures for protection of exchange[91]

[86] Wisconsin Statutes section 166.03 Emergency powers of Governor
[87] Wisconsin Statutes section 252.02(6)
[88] 45 CFR 164. 512 (a) and (b)
[89] Wisconsin Statutes section 146.82(2)(d); 45 CFR 164.528(a) and (b)
[90] Wisconsin Statutes section 252.05(2); HFS 145.04(1) and (2), Wis. Admin. Code; and 45 CFR 164.502(b) "minimum necessary" did not apply
[91] Security and Privacy Rules

- Requirements for receipt of the information[92]

2.10.c 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 oral communication within 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 requester, 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 organizations - a method commonly used to identify employees for the purpose of controlling physical access to a building and then ultimately to patient information. Often these badges contain authorization for accessing certain physical locations within the building. Restrictions on access can be in the form of limited hours or specific areas such as medical records.

[92] Wisconsin Statutes section 252.05(6); HFS 145.04(2)(d)45 CFR 164.501 Definition of designated record set

3 - Patient and provider identification

The representative organizations each used verification procedures for cross-matching identities to verify service providers such as the laboratories. 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 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 use 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 telephone and would release information to law enforcement, hospitals, hazmat teams, or regional media, orally or through a press release, limiting the information released to that 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 spoken messages.

These 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 results 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 oral 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 department 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, 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 these badges contained authorization for access to specific 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 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 by the state lab to the receivers as described above.

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 broad-based authority for exchanging the results of a positive anthrax test as a means to protect public health.

Federal law also requires verification of the requester, 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 driven mainly 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.
   - Upon receipt of information , 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, through the creation of its own case record. This would be supplemented with case investigation material.

2.10.d Critical Observations

Unique to Wisconsin

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

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

Major Barriers to Exchange

No overt barriers were observed. Wisconsin's information-sharing environment allows for easy sharing of information for bioterrorism events. Typically, the minimum amount of information necessary is provided, that is needed to accomplish the purpose, but whenever the public's health is at stake, additional protected health information may be provided.

Documentation of disclosure
Wisconsin law would require the documentation of the disclosure by the state lab. State regulations requiring the documentation of disclosures pose significant barriers to exchange. These 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 the additional step needed 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 only 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.

2.11 Employee Health (Scenario 14)

2.11.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to 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.

2.11.b 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 stakeholders that they would not release this information without patient consent under the facts presented in this scenario. In practice, some of the Workgroup members would require consent to disclose the information to the employer while others would disclose directly to the patient and not require consent. None of the Workgroup members would disclose the information electronically; it would all be done via paper, either mailed or faxed. All would disclose the minimal information necessary to complete the request.

Legal Analysis

State and federal law require patient consent to disclose the patient's medical information related to the back-to-work form from the provider to the employer.[93]

Wisconsin law and the federal privacy law do not require patient 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.[94] Under the Federal Privacy Rule, a provider may require that the request for information from the patient be provided in writing.

Legal Barriers

State and federal law require patient consent to disclose the patient's medical information related to the back-to-work form from the provider to the employer.[95] Some Workgroup members felt that any time consent is required to exchange information it creates a barrier to exchange. The process to share information requires a determination of whether consent is required and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

State law does not require verification of a requester 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 requester of patient identifiable information.[96]

The stakeholders agreed that a "cut and paste" process from the provider's EHR would not be an acceptable process for assembling patient information to be sent to the patient's employer. The Federal Privacy Rule requires that the provider releasing the patient back-to-work information apply the HIPAA "minimal necessary" standard in relation to the information released.[97] The application of this process presents a barrier to health information exchange.

[93] Wisconsin Statutes section 146.82(1), 51.30(4)(a), 252.15(5); 45 CFR 164.508
[94] Wisconsin Statutes section 146.83, , 252.15(5)(a); 1HFS 92.05; 45 CFR 164.524
[95] Wisconsin Statutes section 146.82(1), 51.30(4)(a), 252.15(5); 45 CFR 164.508
[96] 45 CFR 164.514(h)(1)
[97] 45 CFR 164.514(d)

Both state and federal law requires documentation of a disclosure to the patient's employer.[98] Only state law requires documentation of disclosure to the patient.[99]

This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

An additional barrier to health information exchange identified in this scenario relates to security of information transfer and transmission. If the HIPAA Security Rule applies to the discloser of information from the health care provider to the employer, the method and means of exchange would be required to be secured.[100]

2.11.c 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 to complete a 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

Business practices vary as to the extent of documentation of the release of "return-to–work" information 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

[98] Wisconsin Statutes section 146.82(d),; 45 CFR 164.528
[99] Wisconsin Statutes section 146.83
[100] Security and Privacy Rules (HIPAA)

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 law and federal law require 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. Consent is not required for release of information directly to the patient.

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

Wisconsin 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 as part of 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 the "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 disclosures to the patient or the employer, but compliance with these policies is variable.

2.11.d 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 they 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 for the consent vary and therefore most consent forms used in Wisconsin satisfy both requirements. Both obtaining consent and Wisconsin-specific requirements for the consent constitute barriers to exchange.

Documentation of disclosure
Wisconsin 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.

2.12 Public Health (Scenarios 15–17)

2.12.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to 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.

2.12.b 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 law, State A would disclose personal health information to State B without patient consent in this scenario. The state would contact the local public health department, which 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 identified for the public health scenarios. Wisconsin's information sharing environment allows for the sharing of information for mandatory reporting and disease containment for public health purposes, such as for communicable diseases.

Typically, the minimum amount of information necessary is provided to accomplish the intended purpose, but whenever the public's health is at stake, additional protected health information may be provided without patient consent as needed.

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 contacts (in this scenario, the patient's fellow passengers).

Legal Analysis

State and federal law either mandate or allow disclosure of the confirmation of a communicable disease such as tuberculosis (TB) without 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.[101] According to Wisconsin Statutes section 252.03(2), local health officers may do what is reasonable and necessary for the prevention and suppression of disease; according to Wisconsin Statutes section 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 Statutes chapter 252. According to Wisconsin Statutes section 252.02(6), the Department may authorize and implement all emergency measures necessary to control communicable diseases, including TB. This statute also requires physicians, health care facilities,

[101] HFS 145.04(2) (d), Wis. Admin. Code

and laboratories that know or have reason to believe that a person treated or visited by him/her has a communicable disease, has died, and shall immediately report to their local health officer. The local health officer shall report this information to DHFS.[102] The powers defined in this statute allow the removal of barriers to allow rapid and effective responses to a TB threat. Local health officers have powers similar to those of the Department; however, they need to keep the Department updated of measures taken. In addition, Wisconsin is part of an informal group of states (Greater Board of Health Initiative) which will share data interstate, in the event of communicable disease outbreaks.

Wisconsin also has a public 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, U.S. mail, etc., to all health care providers and public health agencies to help them understand the threat and alerted them to possible cases. This communication most likely will not identify patients by name; however, it may contain other elements of protected health information such as demographic characteristics, age, gender, etc. However, if identifying the patient is necessary to help find TB cases, then the patient's identity would probably be disclosed. Wisconsin law will allow this and the decision is based on balancing of patient privacy versus protecting the public. In Wisconsin there are no privacy barriers to prevent exchanging this information.[103]

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.[104]

Neither state nor federal law presents privacy barriers such as requiring patient consent to the disclosures within this scenario.

This scenario did not present an information exchange in which there is a request for information, so the requirement for verification of the requester did not need to be met in this scenario and did not present a barrier to information exchange.

The scenario also did not present a barrier in relation to the determination of information to be disclosed. The State is granted broad powers of authority to maintain and control communicable disease and would be enabled to disclose information as deemed necessary. The federal law, although applicability to this scenario is questionable, does not apply the "minimum necessary" standard to disclosures required by law.[105]

Legal Barriers

State and federal law requires the documentation of disclosures within this scenario, although the stakeholder practices were variable.[106] Wisconsin law requires the Department to maintain reports of communicable diseases as health care records under Wisconsin Statutes section 146.81-.835[107] and therefore disclosure of information from reports would require documentation of the disclosure under Wisconsin Statutes section 146.82(2)(d). If the state authority in this scenario is a HIPAA-covered entity then the Privacy Rule would also require documentation of the disclosures to meet the patient's right of

[102] HFS 145.04(2)(d), Wis. Admin. Code
[103] Wisconsin Statutes section 252.02(6)
[104] 45 CFR 164. 512 (a) and (b)
[105] 45 CFR 164.512(a); 45 CFR 164.502(b)(2)(v)
[106] Wisconsin Statutes section 146.82(2)(d); 45 CFR 164.528(a) and (b)
[107] Wisconsin Statutes section 252.05(6)

accountability.[108] This requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

An additional barrier to health information exchange identified in this scenario relates to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, the federal requirements relating to a secured method of information exchange and security measures for protection of the exchange[109] would need to be met and would present a barrier to the exchange of information.

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 for screened candidates. The State has the authority to conduct the test and to 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 – it may contact the specialty care centers. The state lab maintains a registry, which is mandated by Wisconsin law; however, the registry has an "opt-out" provision: parents of children with positive screening results may sign a form and opt out of the 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 results to the state lab. The State can also disclose to local public health departments without patient consent.

Legal Analysis

Wisconsin law allows disclosure of state-mandated newborn screening test results to the state lab, to the child's physician and family, to specialty care centers providing specialized treatment for the screened anomaly, and to the state health department without patient consent. Wisconsin law also mandates the Department to establish and maintain a registry for identified birth defects as depicted in this scenario.

Wisconsin law requires screening for congenital disorders of all newborns; screening samples are to be submitted and processed through the Wisconsin State Laboratory of Hygiene ("state lab") (Wisconsin Statutes section 253.13). This scenario presents a similar process to that authorized by Wisconsin law.

[108] 45 CFR 164.528
[109] Security and Privacy Rules (HIPAA)

Wisconsin law mandates disclosure of the screening result from the state lab to the physician [Wisconsin Statutes section 253.13(4)], and the HIPAA Privacy Rule allows disclosures without patient authorization when a use/disclosure is required by law, for public health activities or for treatment purposes [45 CFR 164.512(a) and (b); 45 CFR 164.506].

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

The state lab is contracted to perform the necessary diagnostic services and tests on behalf of the Department so exchange between these entities would be allowed by law without patient consent.[110]

The Department has an obligation under Wisconsin Statutes section 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 under Wisconsin Statutes section 253.12 (3)(a)1.d. and Wisconsin Statutes section 253.13(4) and (5). The State agency may notify the physician and the patient's family of eligibility for state programs; however, the patient/family may opt out of this notification [Wisconsin Statutes section 252.13(3), (4) & (5)]. In Wisconsin, the disclosures relating to referral for treatment are made to the provider and patient's family, and generally not disseminated to specialty care centers except when the Department is involved in a specific referral for treatment. A general disclosure to multiple specialty care centers without a more specific referral may require patient consent.

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

There is no requirement or continuing allowance for follow-up by the state registry to a physician [Wisconsin Statutes section 253.13(3)(a)1]. State law does, however, allow for disclosure by a physician to a state agency that is determining a duly authorized function without patient consent, upon the receipt of a written request [Wisconsin Statutes section 146.82(2)(a)5]. HIPAA (45 CFR 164.512(b)) would also allow disclosure by the physician to the state registry for public health purposes without patient authorization.

There are no privacy barriers, such as requiring patient consent, related to the disclosures within this scenario.

This scenario did not present an information exchange in which there is a request for information, so the requirement for verification of the requester did not need to be met in this scenario and did not present a barrier to information exchange.

Legal Barriers

State and federal law requires the documentation of disclosures within this scenario[111] although the stakeholder practices varied. Wisconsin law would require the physician to document disclosures to the

[110] Wisconsin Statutes section 253.13(2)
[111] Wisconsin Statutes section 146.82(2)(d);); 45 CFR 164.528(a) and (b)

patient or patient representative and to the state registry. State law would also require the state laboratory, as a health care provider, to document disclosures made without consent to the physician and the specialty centers.[112] HIPAA also requires covered entities to document disclosures made so that an accounting of disclosures is available to the patient.[113] These documentation requirements present barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

The federal Privacy and Security Rules require that the identity of a requester for protected health information be verified to determine that individuals are who they claim to be. In this scenario, the physician as a covered entity under HIPAA would be required to verify the requester from the state registry tracking the patient through the registry process. This requirement presents a barrier to health information exchange.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, the following requirements would need to be met and will present barriers to the exchange of information.

- Determination of information to be disclosed[114]
- Method of exchange and security measures for protection of exchange[115]
- Requirements for receipt of the information[116]

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 (more detailed information is required for disclosure) and a specific timeframe (e.g., only applies for one year). Sensitive health information requires more consent and documentation to release information, even for treatment purposes. Additionally, interpretation of the legal requirements varies. Most agencies err on the side of being too protective of patient information so as not to release information incorrectly.

[112] Wisconsin Statutes section 146.82(2)(d)
[113] 45 CFR 164.528
[114] 45CFR 164.502(b) "minimum necessary"
[115] Security and Privacy Rules (HIPAA)
[116] Wisconsin Statutes section 253.13(4); 45 CFR 164.501 Definition of designated record set

The exchange of general information between the primary care provider and the drug addiction center for treatment purposes does not require patient consent. Some of the 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 differing interpretation and application of state and federal law.

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

By law, the disclosure to the relative requires patient consent. 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 privacy and security, as well as 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 barriers 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.

The request for information from the shelter was a complicating issue in this scenario. 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.

The "minimum necessary" standard would not apply to information exchanges for treatment. It would be appropriate to apply this standard to all other exchanges in this scenario and all stakeholders did so.

Legal Analysis

State and federal law require an exchange-by-exchange analysis in this scenario to determine whether or not the requested information may be disclosed with or without patient consent. This scenario clearly depicts the complexities of the health information exchange process in Wisconsin. It requires determining who is requesting the information, whether they are who they say they are, whether they have the authority to access the information, what law applies, whether the information exchanged is sensitive, what should be disclosed if the information is releasable, and what additional restrictions apply to the mode and security of the exchange.

The process for information exchange in this scenario required the application of at least four laws and an administrative code, including the HIPAA Privacy and Security Rules, the federal rules regulating alcohol and other drug abuse, Wisconsin Statutes section 146.82, Wisconsin Statutes section 51.30 and Wisconsin Administrative Code HFS 92. The application of that analysis to these exchanges, understanding there are very specific constraints under Wisconsin law, allows disclosure from provider to provider of non-sensitive patient information without consent. The disclosure of sensitive information from the drug treatment clinic to the county for reimbursement purposes and to the county homeless shelter for

verification of treatment was allowable without consent under the state and federal privacy rules[117] but consent was required by the rules regulating alcohol and other drug abuse treatment records.[118]

Legal Barriers

The federal regulations controlling records related to alcohol and other drug abuse provide very restrictive privacy protection to sensitive patient information. These regulations preempt both state and federal privacy rules in requiring patient consent for disclosures to the county for reimbursement purposes, and to the county homeless shelter for verification of treatment. The complexity of this analysis, the variability in the application of the laws, and variability in current practices present significant barriers to health information exchange of sensitive patient information.

This scenario also presented an opportunity to review access to patient information by the family. In this case, analysis of state and federal law clarified that patient consent is required to release patient information to the patient's family.[119] HIPAA would have allowed disclosure to the family members if they were involved with the patient's care and the patient agreed, but these facts were not present in this scenario and HIPAA was preempted by state and other more protective federal law.

Anytime consent is required to exchange information, it creates a barrier to exchange. The process to share information requires a determination of whether consent is required, and the analysis presents a barrier to health information exchange. The process to obtain consent poses an additional barrier to exchange because it requires contact with the patient or other legally authorized person to obtain the consent. Additional barriers include determining who is legally authorized to sign the consent and validating the statutorily required elements of the consent.

The federal Privacy and Security Rules require that the identity of a requester for protected health information be verified to determine that individuals are who they claim to be. In this scenario, if the county homeless shelter, either by contract or by definition, is governed by HIPAA Privacy and Security laws, verification of the family member requesting the patient information would be required. This requirement presents a barrier to health information exchange.

Although HIPAA would not require documentation of disclosure for treatment and payment purposes[120] as depicted in this scenario, Wisconsin Statutes section 51.30 requires documentation of disclosures made by a health care provider so when applicable in this scenario, such as from the substance abuse facility, documentation would be required. This documentation requirement presents barriers to health information exchange by requiring specific documentation of a disclosure every time a designated disclosure occurs. Although this requirement may be met by audit and monitoring techniques in an electronic exchange, the electronic system will be required to document the statutorily required elements.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario, the following requirements would need to be met and will present barriers to the exchange of information:

[117] Wisconsin Statutes section 51.30(4)(b)2; Wisconsin Statutes section 46.215, 46.22, 51.42 or 51.437; 45 CFR 164.506
[118] 42 CFR Part 2
[119] Wisconsin Statutes section 51.30(4)(b): 45 CFR 164.512 and 164.508; 42 CFR Part 2
[120] 45 CFR 164.528(a)(1)(i)

- Determination of information to be disclosed and application of the "minimum necessary" standard[121]
- Method of exchange and security measures for protection of exchange[122]
- Requirements for receipt of the information[123]

2.12.c Domains

The Variations Workgroup identified the following domains as relevant to scenarios 15-17:

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, except in public health communities where the requester is 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 information, as in Scenario 17, a written request for patient information would be required to indicate the information needed and to verify the requester. 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 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 requester for requests related to mental health, alcohol and other drug abuse and developmental disabilities. Among stakeholders queried for these scenarios, there is wide variation in verification practices.

All stakeholders listed incorporated the following into their organizational policies and procedures:

- Nearly all stakeholders use some form of physical identification within their organizations. Often these badges contain authorization for accessing certain physical locations within the building. Restrictions on access can be in the form of hours of the day, physical location of medical information and isolation units that can be accessed. Different methods are used to limit authorization.

[121] 45CFR 164.502(b) "minimum necessary"
[122] Privacy and Security Rules (HIPAA)
[123] Wisconsin Statutes section 51.30; 45 CFR 164.501 Definition of designated record set

- 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 to information.

2 – Information authorization and access controls

When receiving a request for health information, all relevant stakeholders 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 these badges contain authorization for accessing certain physical locations within the building. Restrictions on access can be in the form of hours of the day, physical location of medical information, and isolation units that can be accessed. Different methods are used to limit authorization.

Public health agencies typically do not have a way to limit physical access to their records, but access is typically 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 systems 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 to 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 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 identity when mandatory conditions are reported. Often there is a form that is used to follow up that requires more specific information from the 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.

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 fax, and responses to these requests 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 such information is released only for treatment purposes, and even then only the information relevant to the care being received. In the case of mental health information, 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 oral 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 the patient's family, generally s/he will schedule an appointment with the family and tell them the results in person. In the event that a primary physician cannot be identified, the local public health agency will be contacted to provide these results to the patient and the patient's family.

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 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 systems 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 to 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.

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 medical records clerks, the following information is logged: requester 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 records system, 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 access is typically 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 these badges contain authorization for accessing certain physical locations within the building. Restrictions on 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, which are more restrictive for records containing sensitive information.

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 provided the opportunity to opt out of the exchange only 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, by mail, or by fax (based on the circumstances).

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

2. Documentation of disclosure.

   Wisconsin 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 provided the opportunity to opt out of the exchange only 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, by mail, or by fax (based on the circumstances).

In the event of a medical emergency, the requester 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 records system, 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; 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.

2.12.d Critical Observations

Unique to Wisconsin

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

Wisconsin requirements for documentation of disclosures related to this more sensitive information are also often more stringent than federal law, 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.

Anytime 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.

Consent is required by law in Wisconsin for the exchange of sensitive information unless the disclosure meets one of the very specifically defined and rigid exceptions. Wisconsin law is also more stringent than federal law, which results in barriers to exchange across state lines. The requirement for 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 (on mental health and alcohol and other drug abuse) also requires verification of the requester, 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 the "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 only 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 privacy and security 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 information collected by a mental health professional?

Consent and documentation of the release of information create the biggest barriers to the exchange of information in these scenarios. For 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.

2.13 State Government Oversight (Scenario 18)

2.13.a Stakeholders

The following stakeholders from the Variations Workgroup contributed to 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.

2.13.b 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 no 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 as permitted by law, but cannot send the information to a state university faculty without a business agreement.

Legal Analysis

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, patient consent would not be

required. However, without appropriate statutory authority to share identifiable patient information among state agencies or patient consent, a contractual agreement would be required.

Legal Barriers

In this scenario, the Governor requested state agencies to share identifiable patient information, including Medicaid services data, to determine if children were receiving appropriate health care services. Both federal and state law (Wisconsin Statutes section 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 clear based on the information, provided. An analysis would need to be completed prior to the release of this information and patient consent or contractual agreement may be required. The need for further legal analysis, the complexity of application of the laws, and the variability in practice of rules and regulations applied by multiple state agencies create a barrier to the inter-agency exchange of patient 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 some type of legally authorized contractual agreement such as a business associate agreement. More specifically in this scenario, Wisconsin Medicaid data cannot be disclosed unless there is a business associate agreement in place between the University and the Department; otherwise the disclosures would be in violation of the federal privacy regulation. This disclosure would be regulated by HIPAA Security and Privacy Rules and, in relation to some state agency records, Wisconsin privacy rules and would require a business associate agreement between the entities to share/exchange identifying patient information. The requirement for a legal agreement to exchange would impose a barrier to information exchange.

Additional barriers to health information exchange identified in this scenario relate to security of information transfer and transmission. If the HIPAA Security Rule applies to any of the disclosers of information in this scenario the following requirements would need to be met and will present barriers to the exchange of information:

- Determination of information to be disclosed and application of the "minimum necessary" standard[124]
- Method of exchange and security measures for protection of exchange[125]

2.13.c 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

[124] 45CFR 164.502(b) "minimum necessary"
[125] Security and Privacy Rules

1 - User and entity authentication

To verify the requester, 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 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 for a business associate agreement is defined and regulated by federal law. The agreement must 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

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 without patient consent between state agencies performing a legally authorized function. Wisconsin law requires 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 university[126]

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.

2.13.d 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 expected 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 (e.g., schools, Medicaid, public health, etc.).

[126] Wisconsin Statutes section 146.82(a)

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 requester for health information, a secured electronic transmission and the application of the "minimum necessary" standard for disclosure (unless for treatment). All these processes would present a barrier to open information exchange.

Consent
Wisconsin state and federal law require patient consent to disclose patient 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 obtaining the consent and the Wisconsin-specific requirements for the consent serve as barriers to exchange.

Documentation of disclosure
Wisconsin 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 varies, the requirements to document the release of information pose a barrier to exchange.

2.14 Summary of Critical Observations and Key Issues

A barrier to health information exchange (HIE) is defined as anything that impedes health information exchange. A barrier might prevent exchange of certain information, or could add steps to the process, thus slowing the exchange. Barriers identified through the evaluation of the 18 scenarios were often business practices, policies or laws.

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 the Variations and Legal workgroups and will serve as a starting point for the Solutions Workgroup.

2.14.a Barriers driven by law

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

During the analysis of the 18 scenarios, both the Variations and Legal workgroups identified laws that create barriers to health information exchange within the scenarios. These included:

- Requirements for verification of requesters for health information
- Requirement of a patient consent/authorization before exchange is allowed
- Lack of a statutory exception allowing information exchange without patient consent
- Differing treatment of health information depending on type, source, location
- Strict technical requirement for securing information during the exchange
- Limitations on access to those involved in the information exchange process
- Limitations on the information that could be exchanged once approved for exchange
- Burdensome requirements for specific documentation of information disclosed/exchanged
- Requirements on receipt and retention of information received during an exchange

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 law, then those posed by both state and federal law and finally the barriers posed solely by federal law.

2.14.b Barriers driven by Wisconsin law

Treatment of mental health, alcohol and other drug abuse and developmental disability information
Wisconsin law treats information relating to mental illness, developmentally disabled or alcohol and other 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 greater protection than general health care information in Wisconsin and greater protection than provided in the HIPAA Privacy Rule. The result of this more stringent protection is often the requirement that patient consent be obtained, which creates a barrier intra- and inter-state to information exchange. For example, Wisconsin Statutes section 51.30 requires patient consent to disclose information for treatment or payment purposes. Federal law allows these disclosures for treatment purposes without consent, which creates more of a state barrier to national exchange because Wisconsin has different regulations than federal law and other states. Furthermore, because, current technology in general 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 law, which further increases the barrier because these elements differ from federal law and likely from required elements in other states.

Treatment of HIV Test Results
Wisconsin law also treats HIV test results as "sensitive" information and provides more stringent privacy protection. However this statute is more consistent with state protection of general health care information and the HIPAA Privacy Rule, so it creates less of a barrier to health information exchange than does Wisconsin Statutes section 51.30. For example, this Wisconsin law allows the exchange between providers without patient consent for treatment purposes, although 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.

Minimum necessary
State requirements relating to mental health, alcohol and other drug abuse and developmental disability allow only the "minimum necessary" information to be exchanged. 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 only the "minimum necessary" is exchanged is also time-consuming, creating a barrier to exchange.

Variability in how the standard is applied creates an additional barrier.

Documentation of disclosures
Wisconsin law requires the documentation of disclosures made with or without patient consent. This documentation requirement is deemed a significant barrier to health information exchange as it requires documentation for every health information disclosure. Documentation requires several elements that vary slightly depending on whether the information is sensitive or non-sensitive. In practice, compliance with the law varies; however, the 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, reducing the impact of this 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 law mandates verification of the requester of health information related to mental health, alcohol and other drug abuse and developmental disability, but does not require verification for the disclosure of general health information. This process effectively blocks information exchange until this requirement has been met. 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 an additional barrier to exchange. This statutory requirement effectively prohibits a provider who receives health information through an exchange from allowing that information to continue to be exchanged from the receiving site.

Privat-0 pay patients opt out of research
Despite the benefits of controlled and secured research processes to patient care, current patient privacy statutes allow private-pay patients to opt out of research projects. This opt-out process may ultimately result in a barrier to information exchange for research purposes.

2.14.c Barriers driven by Wisconsin state and federal law

Consent
Anytime consent is required to exchange information, it creates a barrier to exchange. The process to obtain 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.

Whenever either state or federal law is deemed more protective and requires a patient consent for information exchange, obstruction to exchange will occur.

The consent process requires coordination of both 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.

2.14.d 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 gives no guidance as to how to perform verification, so practices are variable; this creates additional barriers to the exchange of information.

Minimum necessary
Federal requirements to limit the exchange of health information in certain types of disclosures to the "minimum necessary" standard, only releasing what is necessary to fulfill the request, increase the amount of time required to exchange health information and limit 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 only the "minimum necessary" is exchanged is also time-consuming, creating a barrier to exchange.

Variability in how the standard is applied 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 for 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 health care 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 complying 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 law does not regulate what it considers "uses" of information that are not disclosures. These are often internal exchanges where information is 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 creates a barrier to information exchange. In the scenarios, in cases where Wisconsin law would not regulate an internal use, federal law would be followed. These additional federal restrictions create barriers to information exchange in Wisconsin.

2.14.e 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 consent 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 often does not 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 requester results in barriers to efficient exchange of patient information.

Allowed access
There was great variability in who would be allowed access and the amount of information accessible. This variability creates significant barriers to information exchange.

Method of disclosure
The method of disclosure varied greatly among the stakeholders, and included fax, phone, mail and electronic exchange. These 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 exchanges to remove the responsibility for security.

Information to be Exchanged
There was significant variability in the information that would be exchanged once the exchange was approved. Some facilities would exchange all patient information and some very specific, limited information. This variability creates significant barriers for information exchange.

Receipt of Information
There was significant variability in how exchanged information is treated and assimilated when received.

Technology
All of the stakeholders with EMRs who stated they would not allow external access to their health records said they would allow access if their technology allowed them to limit access to only relevant parts of the record and to only 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 systems, the technology or lack thereof creates a barrier to exchange. For those who do not have electronic medical records systems, paper records themselves create a barrier to exchange.

2.14.f 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.

Variations 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 the 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 improve 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. The group believes that without advances in technology, we cannot have effective HIE.

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

Second, 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.

Section 3.0 – Summary of Key Findings from the Assessment of Variation

3.1 Main Finding from the Interim Assessment of Variation Report

The Variations Workgroup assessed current policies and practices in health information exchange within the context of the 18 scenarios provided by RTI. The practices are commonly referred to as information disclosure practices and include practices related to both paper and electronic disclosures. The assessment resulted in a detailed understanding of current business practices associated with the exchanges of information presented in the scenarios. Through the review of practices by all stakeholders, wide variations in information exchange practices among stakeholders were identified. Further review provided insight into which practices facilitated the exchange of information and which impeded exchange. The impeding processes were identified as barriers to health information exchange. Additional analysis provided the opportunity to look at each barrier and assess whether the barrier was necessary to provide privacy protection for health care information or an unnecessary impediment to quality patient care. The Legal Workgroup reviewed the variations, barriers and exchanges to determine which barriers were a result of law vs. business policy or practice.

Each of the barriers identified in the Variations Phase was presented to the Solutions Workgroup to determine if it should remain or be reduced or eliminated.

This section describes the major barriers identified by the Variations Workgroup that were presented to the Solutions Workgroup. The barriers were not prioritized by the Workgroup; therefore we have included every barrier identified by the Variations Workgroup because each identified barrier was presented to and discussed by the Solutions Workgroup. Once solutions were developed and refined in later project phases, the solutions were prioritized based on feasibility and impact. However, at the early stages of the project, they were not prioritized.

The barriers were organized by the driver of each barrier to provide an organized approach to finding solutions. They were presented in this manner to the Solutions Workgroup:

- Barriers driven by Wisconsin law
- Barriers driven by both Wisconsin and federal law
- Barriers driven by federal law
- Barriers driven by policy and practice

3.1.a Barriers driven by Wisconsin law

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

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

- Consent for specific types of disclosures (payment and treatment)
- Verification of the requestor for this information
- Minimum necessary

HIV test results are also treated as sensitive information (Wisconsin Statutes section 252.15), except that they can be disclosed from provider to provider for treatment purposes.

Other barriers driven by Wisconsin law include:

- Documentation of all disclosures made with or without patient consent, including as defined in Wisconsin Statutes chapter 146
- Requirements prohibiting re-disclosure of health information
- Consent requirements more stringent than federal requirements, such as for disclosure to the patient's family
- Required interface between state and federal law requirements

3.1.b Barriers driven by state and federal law

Whenever state and federal law do not mirror one another, several barriers to the exchange of information are created. First, one must determine which law controls (state or federal), then once the controlling law is determined, one must understand the requirements of the controlling law. This makes inter-state exchange of information increasingly difficult because other state laws must be understood in order to exchange.

Consent requirements, governed by both state and federal law, present the greatest hurdles to health information exchange. The barriers are caused by:

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

Although eliminating these consent requirements would reduce the barriers to exchange, federal law 42 CFR Part 2 requires patient consent to exchange alcohol and other drug abuse information for treatment purposes unless revision of that federal law occurs.

Other areas where state and federal law differ include:

- The "minimum necessary" standard
- Verification of requester
- Requirement for provision of Notice of Privacy Practices

3.1.c Barriers driven by federal law

In some cases, 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 identified by the workgroups that pose barriers to exchange include:

- Requirements for business associate agreements
- Federal Privacy Rule requirements, including patient rights
- Federal Security Rule requirements

3.1.d Barriers driven by policies and practices

The Variations and Legal workgroups identified several barriers to HIE that are driven by policies and practices. Most often, variation in policy and practice implementation led 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
- Method of retention
- Variability in the implementation of the law

The final barrier to exchange identified by the workgroups is technology. In general, current technology used in Wisconsin cannot limit access to relevant parts of the record or to specific records to comply with "minimum necessary" requirements. Furthermore, currently employed technology often cannot specify the type of access (read-only, edit/modify, delete) granted to the user.

For those entities that do not have electronic health records, the lack of technology creates a barrier to exchange. Many workgroups working to inform Wisconsin's eHealth Care Quality and Patient Safety Board identified the cost of implementation of electronic health records as the major impediment to health information exchange. Therefore, one of the greatest hurdles to HIE is the cost associated with universal adoption of electronic health records. Funding will need to be provided to many providers in order to implement technology.

3.2 Effective practices

In reviewing the 18 scenarios provided by RTI and engaging in numerous discussions regarding the exchange of health information, many effective practices were identified that position Wisconsin to be a leader in health information exchange. Many of these practices drastically improve organizational ability

to exchange health information, particularly in relation to exchanging for treatment purposes. Generally, these practices would translate to an electronic environment.

Effective practices identified in the Variations Phase include:

- Exchange between providers for treatment without patient consent except for sensitive information protected by Wisconsin Statutes section 51.30.
- Segregation of all sensitive information (governed by Wisconsin Statutes section 51.30) contained in records to build an exchange for the information that is allowable to be shared without patient consent.
- The integration of received patient information in a manner that allows all patient information to be exchanged so complete and accurate patient information is made available to providers for treatment.
- Internal exchanges for quality assurance and patient education (marketing) purposes; these are "uses" rather than "disclosures" (which require more restrictions).
- Standardized processes for verification of requester.
- Not utilizing the "minimum necessary" standard for disclosures provider-to-provider for treatment.
- Creation and maintenance of a database containing known providers and health agency users with their contact information for identifying the agency requesting information.
- Consistently employing a standardized model for role-based access for electronic medical records systems.
- Implementation of a standardized written business associate agreement, which allows for the exchange of information. (This can also hinder exchange, because it requires the legal document prior to exchange.)
- The added flexibility provided to public health for exchanging information as needed in order protect the interests of the public.

3.3 Lessons learned

Not only did the Variations Workgroup identify best practices through evaluating variations in business policies and practices associated with exchanging health information, but it also identified areas in which improvements must be made in order to improve the exchange of information. The greatest improvements will be required in technology and law.

This section describes the lessons learned or areas which need to be improved to allow better exchange of health information in Wisconsin.

3.4 Health information technology and exchange

While Wisconsin is a somewhat rural state, Wisconsin is in a unique position to move forward with health information exchange due, in part, to the following:

1. The large number of physicians in large group practices.
2. Many larger groups and hospitals have implemented or are currently implementing electronic information systems.
3. Many of the systems in place in Wisconsin are already interoperable or are maintained by the same vendor (e.g., EPIC).

4. The number of organizations that are engaged in health care quality improvement.
5. The engagement of Metastar in the DOQ-It program, enabling small physician practices the opportunity to receive resources to enhance the transition from paper to electronic information systems.
6. The creation and implementation of the Wisconsin *eHealth Action Plan.*

Nevertheless, this will be an incremental process. For the most part, almost half of the Variations Workgroup members indicated that they were not using electronic systems to record or exchange patient information except for billing purposes. The organizations that were using electronic medical records systems were generally not exchanging health information through electronic means or were only exchanging within a networked health care system. In these organizations, additional resources were needed to incorporate all incoming information from outside organizations into the medical record through a manual process. For one of the stakeholders, information can be accessed by their business associates through a web-based query method, but this information cannot be directly incorporated in another organization's electronic system. The Governor's mandate to have electronic health care systems exchanging information in five years is a noble goal and one that is currently engaging stakeholders, consumers, providers and patients in transitioning to more efficient health care information processes.

Many policies and procedures currently in place could be used in an electronic environment without too much difficulty. Technology provides the means to overcome many security and privacy barriers, but technological innovations cannot overcome all barriers that exist primarily because of restrictive statutory language. Unless changed, these statutory barriers will continue to present challenges as statewide and national implementation of health information exchange occurs. The advent of health information exchange presents issues related to information integration, accountability, re-disclosure and documentation that have yet to be resolved.

3.5 State and federal law

The lack of standard application and interpretation of state and federal laws is a major driver behind all of the barriers identified through the Health Information Security and Privacy Collaboration (HISPC) process. As a result, "workarounds" are prevalent. Sometimes this means that the state or federal law is interpreted in its broadest sense and sometimes in its most restrictive sense. In some cases, the Workgroup members would like to retain the flexibility they currently have to ensure that the patient's information is protected. For example, "minimum necessary" is a key issue where variation exists. Health information managers have the flexibility to determine what information is disclosed under this provision, allowing them to modify requests based on the need identified. One challenge this presents is that there is no standard expectation for the set of information that health care providers caring for patients can expect when "minimum necessary" applies.

In discussing these situations with stakeholders, it was apparent that health information managers take protection of patient information very seriously. Liability issues force them to comply with the rigid protection of the law when exchange may be in the best interest of patient treatment. They are therefore unable to compromise information security for the sake of rapid exchange of information. In addition, there are many advocates and consumers who want to retain the added protection afforded by Wisconsin law for sensitive health information, such as mental health records and HIV test results. Retention of protective barriers such as consent requirements for release of more sensitive information effectively prohibits open exchange of patient health care information between providers for treatment purposes.

As the discussion moves from high-level policy about the exchange of health information to more detailed discussions of actual practice, solutions for making the new electronic environment a reality are not simple. The challenges of transitioning from a paper environment to an electronic environment involve rethinking the workflow, staff skills, resources, habits, and culture of an organization all while functioning within the limitations of the law. Many business organizations' practices are driven by provisions in federal and state law, and in some cases extend beyond what the law technically requires because of liability concerns.

Therefore, the workgroups placed a strong emphasis on reviewing current restrictions on exchange of health information imposed by state and federal law. Workgroups reviewed current restrictions to determine whether or not the barriers imposed by law added necessary privacy protections. For those deemed unnecessary, the workgroups focused efforts on developing solutions and plans to remove the barrier imposed by the law.

Section 4 – Introduction to Analysis of Solutions

The Solutions Workgroup was formed following the Variations Phase of the project. The barriers identified by the Variations and Legal workgroups served as a starting point for this group. The Solutions Workgroup evaluated each barrier, balanced the patient's right to privacy and security in relation to sharing information for a health care benefit, and determined which barriers should be maintained to protect patient privacy and which should be reduced or eliminated. For those deemed an impediment to patient safety and quality of care, the Workgroup developed solutions to reduce or eliminate the barrier while maintaining proper patient privacy protections.

Once solutions were developed, the Workgroup reviewed all solutions and organized them into the following implementable solutions:

- Revise Wisconsin Statutes chapter 146 to mirror HIPAA for specific exchanges.
- Revise Wisconsin Statutes section 51.30 to allow exchange from provider to provider for treatment purposes.
- Improve the identification and verification of patient identity.
- Propose revisions to HIPAA to improve information exchange and the quality of patient care.

The solutions are detailed further in the following sections.

Section 5 – Review of State Solution Identification and Selection Process

5.1 Overall process to develop solutions

Following the completion of the *Interim Assessment of Variation Report*, the Wisconsin Security and Privacy Project team determined that the Solutions Workgroup should include existing members of the Variations and Legal workgroups as well as additional new members to increase representation in advocacy and policy making. These members were chosen to fully represent all of the stakeholder groups

identified by RTI, to achieve a high level of understanding of the identified barriers and to fulfill the charge to fully represent all groups affected by health information exchange.

The goals of the Solutions Workgroup were:

1. To analyze the barriers identified by the Legal and Variations workgroups.
2. To balance privacy and need to know and determine which barriers should be maintained, modified or eliminated.
3. To develop solutions to the barriers to improve the exchange of health information while maintaining privacy mechanisms that protect individual rights.

The Solutions Workgroup began by considering the variations in organizational-level business practices and relevant state and federal laws that affect and/or pose barriers to health information exchange documented in the work of the Legal and Variations workgroups. The challenge to the Workgroup was to seek solutions to perceived or real barriers to HIE that will improve patient care while considering the impact of the solutions on consumer protection and patient privacy.

With 35 diverse members representing a variety of perspectives, the Solutions Workgroup used a multi-faceted approach that allowed participation from all members and captured a variety of viewpoints. Sessions were designed with a series of small break-out groups and large group discussions as well as scenario re-enactments to develop and refine solutions to the identified barriers. Once the initial solutions were developed, the Workgroup evaluated them based on feasibility and impact. This process allowed for critical re-evaluation of the solutions and further development of critical discussions that balanced the need for exchange against the patient's right of privacy in solutions that will have great chance for success in Wisconsin. The results are the prioritized solutions detailed in this report.

5.2 Solutions Workgroup

The Solutions Workgroup comprised 35 individuals who represent organizations in the various stakeholder groups identified by RTI that would be affected by health information exchange and the proposed solutions, as well as individuals with legislative policy, technical, health information management, policy and procedure and legal expertise. Every stakeholder group identified by RTI was represented in the Workgroup. Half of the members previously participated in the Variations and/or Legal workgroups and were extremely knowledgeable about the identified variations and barriers evolving from those workgroups. The new members strengthened Solutions Workgroup expertise in state agency processes, public health, information management and technology, corrections, minors and varied advocacy issues such as mental health, women's health and health services for the under-served.

The charge of the Solutions Workgroup was to:

1. Identify and develop solutions that reduce or eliminate the barriers identified by the Variations and Legal workgroups while preserving necessary protections to patient privacy and security.
2. Evaluate proposed solutions by assessing:
    a. The impact of the solutions on consumer protection and privacy.
    b. The impact of the solutions on health care organizations' operations and resources.
    c. The feasibility of solutions under current state and federal law.
    d. The relationship of the solutions to national standards.
3. Prioritize proposed solutions and determine which solutions should be further developed.

5.3 Process used to identify solutions

Before the Solutions Workgroup began its work, staff organized an approach to analyze the barriers identified by the Variations and Legal workgroups that proceeded chronologically, so the barriers were approached as they would develop in the health information process. For example, starting with the receipt of an information request and proceed through to the receipt of information. The barriers were then grouped so that each of three Workgroup meetings would focus on a group of barriers while following the chronological approach. The groupings included:

Meeting 1: Method of Request, Verification of Requester, and Verification of Patient

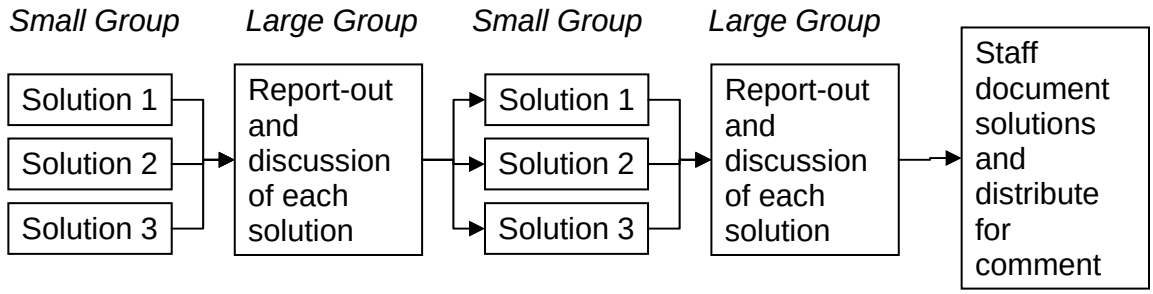
Meeting 2: Patient Consent for Disclosure, Business Associate Agreements, and Exchange of Sensitive Information

Meeting 3: Method of Disclosure, Re-Disclosure, Documentation of Disclosure, and "Minimum Necessary"

Meeting 4 was used to prioritize and refine the prioritized solutions.

Prior to each meeting, participants were given documents that outlined the barriers associated with each topic as identified in the Variations and Legal workgroups. The first part of each meeting was spent as a large group reviewing and discussing the barriers, including discussion of why barriers exist and why some should remain as controls on inappropriate release of information and privacy protection. In one meeting, Workgroup members performed a skit to demonstrate issues with patient consent. In other meetings, the project privacy consultant gave a presentation on the barriers the group would cover at that meeting. Once the barriers were presented, the Workgroup discussed which barriers to address and which ones should be maintained. Barriers determined to be necessary to provide adequate patient privacy protections were reviewed, discussed again, and modified in a manner that allowed them to be re-entered into the proposed solutions.

Once the Workgroup determined which barriers would be analyzed, the Workgroup used a series of small break-out groups, followed by large group report-outs and discussion, to develop solutions to the barriers.



The small break-out groups allowed all individuals on the Workgroup the opportunity to participate in the development of the solutions and also allowed the group to simultaneously work on multiple solutions to maximize the work completed in the short timeframe available. By preparing report-outs to the larger group, small break-out groups were forced to pull thoughts from their discussion into presentable work, receive feedback in the large group discussion and work through the solution again before getting another round of feedback from the large group. In the second round of work, members of the small break-out groups were often mixed to bring additional perspectives and varied stakeholder opinions to refine the solution.

Each solution went through two rounds of development at the Solutions Workgroup meetings. Following the Workgroup meetings, staff documented the solutions and distributed them for additional comment.

5.4 Determination of feasibility of identified solutions

In the final Solutions Workgroup meeting, the group voted to identify the solutions considered most critical to the reduction of barriers to HIE, while considering the feasibility and impact of the solutions. The Solutions Workgroup considered the importance of the removal or modification of the barrier in relation to an improvement in patient care processes as part of the impact of each solution. Each Solutions Workgroup member voted for feasibility and for impact.

The process of voting on feasibility and impact caused the group to change the way they were looking at the solutions. Prior to voting, the Solutions Workgroup had identified several small solutions that corresponded to barriers identified in the Variations Phase. The discussions following the voting led the group to bundle solutions into solution sets that had a strong chance of successful implementation and high impact for Wisconsin. The solution sets were then prioritized by the Workgroup.

Once the critical solutions were identified and prioritized, the group reviewed those with the highest priority. The group used relevant scenarios designed by RTI to create skits to demonstrate the solutions. Each skit was performed as it would be done today; then again as it would be with the solution implemented. A discussion followed. By really seeing the impact of what was being proposed, in some cases, the group decided to alter or add to the solution.

5.5 Organization of identified solutions for this report

In the final meeting of the Solutions Workgroup, the members grouped solutions designed to eliminate or reduce specific barriers into four broader solutions, each of which targeted multiple barriers, in a way that would be simpler to implement.

The four solutions proposed by the Solutions Workgroup are:

- Standardize verification of patient identity
- Amend Wisconsin Statutes chapter 146 to mirror HIPAA in specific areas
- Modify Wisconsin Statutes section 51.30 in relation to information access for treatment purposes
- Propose changes to HIPAA

These broad solutions are described in the next section of the report and organized into categories defined by RTI. The categories defined by RTI and the solutions falling under each category, are:

1. Solutions to variations in organization business practices and policies (section 6)
    - Standardize verification of patient identify
2. Solutions to issues derived from state privacy and security laws/regulations (section 6)
    - Amend Wisconsin Statutes chapter 146 to mirror HIPAA in specific areas
    - Modify Wisconsin Statutes section 51.30 in relation to information access for treatment purposes
3. Solutions to enable interstate ehealth information exchanges (section 6)
    - All four solutions
4. National level recommendations (section 7)
    - Propose changes to HIPAA

Section 6 – Analysis of State Proposed Solutions

6.1 Introduction

This section presents each solution developed by Wisconsin's Solutions Workgroup following the process outlined in the previous sections of this report. The matrix below shows how Wisconsin's proposed solutions fit into the major solution categories defined by RTI. These categories include:

- Solutions to variations in organization business practices and policies;
- Solutions to issues derived from state privacy and security laws/regulations;
- Solutions driven by the intersection between federal and state laws/regulations; and
- Solutions to enable interstate eHealth information exchange.

The first three categories reflect responses to the barriers identified through this project's Legal and Variations workgroups while the final category reflects a key project goal: supporting health information exchange. It is not surprising that each proposed solution is placed in multiple categories.

Section 6.0, Table 1. High-level Roll-up of Solution Categories

Proposed Solutions	Solutions that…			
	Address Variations in Organization Business Practice or Policy	**Address State Law/ Regulations**	**Address the Intersection between State and Federal Law**	**Enable Interstate eHealth Information Exchange**
Change Wisconsin Statutes chapter 146				
Allow Family Access		X		X
Expand Law Enforcement Access		X		X
Remove Re-disclosure Prohibition		X		X
Remove Documentation Requirements		X		X
Change HIPAA				
Eliminate Business Associate Agreements (BAAs)			X	X
Remove Research Waiver Req.			X	X
Clarify "minimum necessary"		X	X	X
Change Wisconsin Statutes section 51.30 (sensitive information)				
Allow Access to Providers for Treatment Purposes		X		X
Standardize Verification of Patient Identity	X			X

6.2 Solutions to variations in organization business practices and policies

'Solutions to variations in organization business practices and policies' is the first major solution category outlined by RTI. This category includes five sub-categories:

- Governance-related solutions;
- Business arrangement solutions;
- Technical solutions;
- Guidance/education solutions that address misinterpretation issues; and
- Business agreements, and uniform patient consent/authorization forms.

One solution proposed by the Workgroup falls under this major category: standardizing methods to verify patient identity. As indicated in the matrix below, this solution addresses many sub-categories within variations in practices and solutions identified by RTI. Moreover, it is likely to affect organizational governance, and will require both technical standards and policies and procedures for successful implementation.

Section 6.1, Table 2. Solutions affecting variations in business practice or policy (not state or federal law)					
Proposed Solution	RTI Solution sub-categories				
	Governance-related	**Business arrangement**	**Technical**	**Guidance or education for misinterpretation**[127]	**Business agreements, uniform patient consent/authorization forms**
Standardize Verification of Patient Identity	X	X	X	X	X

6.1.a Verification of Patient Identity

CONTEXT FOR PROPOSED SOLUTION: Verification of Patient Identity

Currently, providers do not use a uniform method to capture standardized criteria to identify a patient (patient identifiers).[128,129] Moreover, there is not a standard method to verify patient identifiers at the time of exchange.[130] This lack of standardization creates significant risks to accurate and timely patient care. Variation in practice also poses a number of challenges to exchanging information in a paper or electronic format:

- Criteria used to identify or verify patients in one provider practice might not be utilized or available in another practice;
- Accurate identification of a specific patient is information is difficult and complicated when sending and receiving information;
- Misidentification of patients could lead to medical errors such as the wrong treatment for the wrong patient, inaccurate records for an individual, and inappropriate continuity of care; and
- Misidentification of patients may create liability for inappropriate disclosure.

Moving into an electronic world where information is exchanged between electronic health care systems will require standardized collection of patient identifiers, verification of patient identifiers, and accurate matching of identifiers to patient information.

[127] The project team chose to define 'misinterpretation' broadly to include instances where individuals misunderstand the law as well as instances where individuals understand the law yet interpret it differently.
[128] Capture: The process of collecting patient identifiers from a patient.
[129] Patient Identifiers are information collected from a patient to assist in the identification of the patient (e.g., name, birth date, address, etc.)
[130] Verification: The process of confirming that patient identifiers are correct.

PROPOSED SOLUTION: Verification of Patient Identity

The Workgroup advocates a two-part solution to improve identification and verification of a patient:

1. Create model policies and procedures to ensure appropriate capture of patient identifiers.[131]
2. Adopt nationally defined standards for patient identification once available.

SOLUTION DESCRIPTION: Verification of Patient Identity

The Solutions Workgroup proposes developing a model policy and procedure that includes a standard set of patient identifiers that can be utilized at a state and national level, in a standardized and consistent process, to assure patient identity. This proposal includes a clearly defined approach to ensuring that the components of the model policy are captured, including a process whereby specified identifiers are obtained and reviewed each time a patient receives care or treatment. A standard set of identifiers might also be clearly written on a request for information form or the patient consent form or any other standardized documents used to request patient information to ensure that patients can clearly be identified prior to releasing patient health information.

The Solutions Workgroup recommends creating a future workgroup to refine the standard set of patient identifiers. To assure correct verification of the patient, the Solutions Workgroup recommends that the following identifiers be considered as a starting point for this future workgroup's consideration:

- The patient's full name (the group did not discuss including middle names or honorifics)
- Gender
- Date of birth
- Address
- Zip code
- Phone number

Other additional identification methods might include a driver's license or photograph.

BARRIERS ADDRESSED: Verification of Patient Identity

A model policy and procedure for verification of the patient would greatly increase the ability to correctly identify patients and their information when information is exchanged. This is a useful solution that cold be immediately implemented while waiting for the development of national standards.

With the consistent use of standardized patient identifiers, this solution would greatly simplify the process for identifying a patient, improve the accuracy with which the patient is identified, and decrease the possibility of harmful medical errors. This solution would also lead to significant improvements in

[131] This component of the solution was honed and fine-tuned by the Implementation Workgroup to read: 'Create model policies and procedures to ensure appropriate capture of patient identifiers, verification of patient identifiers, and match of patient identifiers in a health care system.'

patient safety and quality of care, reduce the administrative burden of resolving the identification of patients, and prevent confidentiality violations.

TYPES OF HEALTH INFORMATION EXCHANGE ADDRESSED: Verification of Patient Identity

This solution affects every exchange of patient information involving identifiable patient information.

STAKEHOLDERS AFFECTED AND INVOLVED: Verification of Patient Identity

The grid below indicates the stakeholder groups identified by RTI that have a role in the development of, or are affected by, this proposed solution:

	Section 6.1, Table 1. Stakeholder Group																
	Clinicians	Physician groups	Federal health facilities	Hospitals	Payers	Public health agencies	Community clinics and health centers	Laboratories	Pharmacies	Long-term care facilities and nursing homes	Home Care and hospice	Correctional facilities	Professional associations and societies	Medical/public health schools that conduct research	Quality improvement organizations	Patients, Consumers, Advocacy Organizations	State government
Affected by Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

The impact for accurate identification of the patient impacts all who use or disclose patient information

STAGE OF DEVELOPMENT: Verification of Patient Identity

A number of national organizations are convening experts and building coalitions to address issues surrounding verification of patient identity at the national level. The Confidentiality, Patient Safety, and Privacy Workgroup of the American Health Information Community (AHIC), for example, recently released recommendations regarding patient identity proofing, which they define as 'the process of providing sufficient information to correctly and accurately establish and verify an identity to be used in an electronic environment.' The Markle Foundation's Connecting for Health Initiative devoted an entire policy guide of its Common Framework to 'Correctly Matching Patients with Their Records.'

Wisconsin has not yet initiated a focused effort to develop statewide model policies and procedures. However, Solutions Workgroup members are optimistic that this effort will be supported by Wisconsin's eHealth Care Quality and Patient Safety Board and addressed as one of the eHealth Board's charges in the coming year.

EXTENT SOLUTION IS IN USE: Verification of Patient Identity

No standard approach to verifying patient identity is in use today. Each organization has its own set of processes for verification of patient identity and specific patient identifiers to ensure the appropriate

identification of patients, but in order to exchange information, the identifiers must be standard across organizations that share information.

SCALABILITY: Verification of Patient Identity

This solution affects all individuals and organizations that exchange health information and is applicable in every setting in which information is exchanged. It could be implemented statewide initially but would be much more effective if scaled to the national level. The state model policy could be utilized at a national level until specific national patient identifiers are developed. The adoption of national uniform standards would greatly improve exchanges of information at a national level.

POSSIBLE BARRIERS: Verification of Patient Identity

In order for the solution to be effective, every individual and organization that exchanges health information would have to adopt the model policies and procedures and designated uniform standards. In addition, vendors would have to be aligned to develop products that comply with these standards. Similarly, a large effort would be required to conform legacy data to the new standards. Consistent training on new standards would be critical to ensure that current data not only has the required elements, but also is obtained and/or reviewed each time a patient is treated. Processes and policies in these areas and others would need to be changed and the model policies and procedures adopted at the institution level to support the standards.

DOMAINS ADDRESSED: Verification of Patient Identity

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 – Laws
9 – Information use and disclosure policy

6.2 Solutions to issues derived from state privacy and security laws/regulations

'Solutions to issues derived from state privacy and security laws/regulations' is the second major solution category outlined by RTI. This category includes four sub-categories:

- Solutions that would require changes in existing state law/regulation (e.g., drafting model legislation);
- Solutions that would require new laws/regulations;
- Solutions that would address issues of non-compliance with state laws/regulations; and
- Education solutions to address misinterpretations of state laws/regulations.

Two solutions proposed by the Workgroup fall under the category of solutions to issues derived from state privacy and security laws/regulations:

- Amend Wisconsin Statutes chapter 146 to mirror HIPAA in specific areas; and
- Amend Wisconsin Statutes section 51.30 in relation to provider access to information for treatment purposes.

As indicated in the matrix below, these solutions address multiple sub-categories identified by RTI. Each solution requires a change to existing law, and incorporates education efforts to address misinterpretation issues. In addition, the proposal to amend Wisconsin Statutes section 146.81-83 addresses issues of non-compliance with law identified through this project's Variations and Legal workgroups' discussions.

Section 6.2, Table 3. Solutions to issues derived from state privacy and security laws/regulations

Solutions	Solution Sub-categories Defined by RTI			
	Change existing law	**Require new law**	**Address Non-compliance**	**Education to address misinterpretation issues**
Change Wisconsin Statutes chapter 146				
Allow Family Access	X		X	X
Expand Law Enforcement Access	X		X	X
Remove Re-disclosure Prohibition	X		X	X
Remove Documentation Requirements	X		X	X
Change Wisconsin Statutes section 51.30 (sensitive information)				
Allow Access to Providers for Treatment	X		X	X

It is the Workgroup's belief that these changes will reduce barriers to exchange caused not only by the law, but also by varying interpretations of the law. Moreover, these changes will lead to improvements in the quality of patient care.

6.2.a Amend Wisconsin Statutes chapter 146 to mirror HIPAA in specific areas

CONTEXT FOR PROPOSED SOLUTION: Amend Wisconsin Statutes chapter 146

Following the enactment of a provision for protection of "sensitive" health care information in 1977, Wisconsin Statutes section 146.81-.84 was enacted to protect general patient health care information in 1980. This law was intended to balance the patient's right to have his/her health care information remain confidential with the need for disclosure without patient consent when the legislature determined that societal "need to know" is greater than the patient's right to protection.

Many of the barriers to health information exchange result from strict privacy protection requirements in the current Wisconsin privacy laws. While some of the restrictions clearly interfere with or prohibit information exchange, others are so complex in their application that health care practices relating to disclosures vary greatly among health care providers. The result is often wide variability and inconsistency in disclosure practices. The strictness of the regulations, complexity of interpretation, and variability in practices result in some health care providers allowing disclosure while others deny disclosure. This variability in practice creates significant and often unanticipated barriers to health information exchange.

The federal privacy law, HIPAA, which became effective in 2003, creates many of the same privacy protections at the national level that Wisconsin Statutes chapter 146 affords Wisconsin citizens. Sometimes, however, compliance with two sets of laws creates barriers to health information exchange, notably:

- To exchange health information in Wisconsin, one must first determine which law applies (HIPAA or one of the Wisconsin privacy laws), then determine the statutory requirements for the exchange. For each disclosure, the analysis required to determine whether state or federal law governs the information disclosure process adds complexity.

- When Wisconsin law is more restrictive than HIPAA, the state law supersedes the national HIPAA standards for exchange. Consequently, when someone from outside the state attempts to exchange information with an entity in Wisconsin, he/she has to follow both regulations, and therefore, the exchange is more difficult.

The Workgroup discussed four main areas in which Wisconsin Statutes chapter 146 is more restrictive than HIPAA:

1. Documentation requirements
2. Re-disclosure restrictions
3. Disclosure to family
4. Disclosure to law enforcement

Each of these areas is addressed in the proposed solution.

PROPOSED SOLUTION: Amend Wisconsin Statutes chapter 146

The Workgroup advocates amending Wisconsin Statutes section 146.81-.83 to mirror HIPAA language in the following areas:

5. Expanding disclosures to family[132] (Wisconsin Statutes section 146.82, 146.83)
6. Expanding disclosures to law enforcement[133]
7. Eliminating re-disclosure restrictions (Wisconsin Statutes section 146.82(2)(b))
8. Reducing the documentation of disclosure requirements (Wisconsin Statutes section 146.82 (2) (d), 146.83(3))

SOLUTION DESCRIPTION: Amend Wisconsin Statutes Chapter 146

The section that follows presents each element of this four-part solution in detail, summarizing the topic area as it applies in Wisconsin today as well as the proposed solution.

1. Disclosure to Family (Wisconsin Statutes section 146.82)

Wisconsin Statutes section 146.82 provides no exceptions to its requirement for patient consent that allows for disclosure to families: family members are generally not allowed access to a patient's health information without that patient's consent. Under Wisconsin Statutes section 51.30, regulating "sensitive" patient information, disclosure to families is allowed under certain circumstances without

[132] This component of the proposed solution was adjusted by the Implementation Workgroup to expand access for all individuals involved in the care or treatment of the patient, rather than family members only. This change matches language in HIPAA.

[133] This component of the proposed solution was eliminated by the Implementation Workgroup and, therefore, is not included in the Implementation Plans developed as part of this project.

patient consent.[134] By requiring patient consent to disclose to families, Wisconsin Statutes chapter 146 also differs from federal regulations under HIPAA, which allow disclosure to family members involved in the care and treatment of a patient with that patient's agreement (rather than formal consent).[135] The restrictions within Wisconsin Statutes chapter 146 requiring patient consent to disclose to family members create barriers to the exchange of health information. In addition, differences between Wisconsin and federal laws create additional barriers to exchanges across state lines.

The proposed solution allows Wisconsin (and other states adopting the HIPAA standard) to adopt the national HIPAA Privacy Rule standard for access to protected health information by family members and other individuals involved with patient care, with patient agreement.

This solution would effectively allow family members and others to be more informed and involved caretakers. It would allow providers to share patient information that is deemed important for patient caregivers to know more easily, ultimately benefiting caregivers. Providers would no longer be required to obtain and validate patient consents for family and caregiver discussions.

It should be noted that the Implementation Workgroup further refined the solution to expand access for all individuals involved in the care or treatment of the patient, rather than family members only. This change matches language in HIPAA.

2. Disclosure to Law Enforcement

When comparing Wisconsin's exceptions for access to law enforcement to the exceptions in HIPAA, the state's privacy laws are generally more protective and, therefore, will control. In many cases, this means law enforcement must obtain consent from the patient in order to obtain protected health information (PHI). However, Workgroup members have rarely seen law enforcement provide a patient consent for access. More often, PHI is provided to law enforcement without consent, contrary to state law, or a court order is obtained for the information. This barrier is complicated by the fact that the elements of consent that are required by the state privacy laws vary from those required by HIPAA. In summary, the steps it takes to determine whether or not consent is needed and then which elements are required in that consent pose barriers to the exchange of information. Variations in business practices associated with release of information to law enforcement, ostensibly caused by the complexity of determining which law applies, act as an additional barrier to exchange.

The proposed solution allows Wisconsin (and other states adopting the HIPAA standard) to adopt the national HIPAA Privacy Rule standard for access to protected health information by law enforcement and would provide consistency in approach and implementation of law enforcement access.

This solution would allow law enforcement entities to more effectively perform law enforcement duties that require access to patient health care information (e.g., the investigation of drinking while under the influence, unauthorized drug use, etc.) This solution would, however, reduce existing patient privacy protections.

3. Re-disclosure (Wisconsin Statutes section 146.82(2)(b))

[134] Wisconsin Statutes section 51.30(4)(b)20. allows providers to share a patient's presence in an inpatient treatment facility with family members without patient consent if the spouse, parent, adult child or sibling is directly involved in providing care to or monitoring the treatment of the subject individual.

[135] 45 CFR 164.510(b)

Wisconsin Statutes section 146.82(2)(b) requires that when patient information is disclosed without patient consent, the recipient must keep the information confidential and may not disclose identifying information about the patient. This statutory language effectively prohibits re-disclosure of protected health information (PHI) received without patient consent. That is, when organization A receives PHI from organization B without patient consent, organization B cannot send the information on to (re-disclose to) organization C—with or without patient consent. This prohibition does not apply to PHI received *with* patient consent under Wisconsin Statutes sections 146.83. Wisconsin Statutes section 51.30 and 252.15 regulating sensitive information do not contain re-disclosure prohibitions and allow re-disclosure in compliance with the consent or statutory exception requirements.[136]

Variation in Wisconsin Statutes governing re-disclosure complicates health information exchange in both paper and electronic environments. In order to comply with current law, providers must be able to identify the source of each element of a patient's record prior to disclosing PHI. Patient information received under Wisconsin Statutes section 146.82(b) without patient consent (e.g., disclosure to providers for treatment purposes) cannot be re-disclosed. In contrast, elements received under Wisconsin Statutes section 146.83 with patient consent *may* be re-disclosed. Such variation makes it difficult for the recipient of information to determine whether the received patient information may be disclosed.

The proposed solution allows Wisconsin (and other states utilizing the HIPAA standard) to be consistent regarding re-disclosure of patient information.

Modify the re-disclosure provision would allow providers that are caring for patients more efficient and effective access to patient information. It would continue to provide patient privacy protection by maintaining a requirement for patient consent when appropriate. It would also allow the integration of patient information received such that all of a patient's information may be easily collated and accessible when needed.

4. Documentation Requirements (Wisconsin Statutes section 146.82 (2) (d), 146.83(3))

Wisconsin Statutes section 146.82 (2) (d) and 146.83(3) require documentation of all disclosures of health care information. The Federal Privacy Rule[137] requires documentation of specific disclosures to enable the patient to determine who has accessed that patient's information and when. These statutes vary in when documentation must occur and also what elements are required to be documented. Therefore, in order to document correctly, there must be a determination of what law applies to the disclosure, whether documentation of the disclosure is required, and finally what elements must be documented.

The proposed solution allows Wisconsin (and other states utilizing the HIPAA standard) to adopt the national HIPAA standard for documentation and still enables the patient to determine who has accessed that patient's information and when.

Reduction of the documentation requirements for disclosures would decrease burdensome and costly administrative processes.

BARRIERS ADDRESSED: Amend Wisconsin Statutes Chapter 146

1. Disclosure to Family (Wisconsin Statutes section 146.82)

[136] Wisconsin Statutes section 51.30 covers mental health, alcohol and other drug abuse treatment, and developmental disabilities; Wisconsin Statutes section 252.15 covers HIV test results.
[137] 45 CFR 164.528

Current Wisconsin law does not allow family or other caregiver access to patient information without patient consent. This solution offers a benefit to those involved with the care of the patient to be more knowledgeable and informed while providing care and treatment without having to obtain and validate patient consent.

This solution also eliminates the variance in the state and federal law noted above. These proposed changes are consistent with federal HIPAA regulations, thereby eliminating the variance between state and federal regulations in this regard. If this solution were adopted nationally, it would eliminate inter-state variation as well. Eliminating or reducing these legal variations will minimize the complexity of the process and the variation in interpretation noted above, enhance information exchange and reduce barriers to information exchange processes.

This solution offers additional benefits to providers and recipients of care. It enables family or other caregiver access to patient health information without consent, enabling more informed caregiving. It also increases provider efficiency by streamlining the information release process, and increases the transparency of provider activities to patients, family members, and other designated caregivers.

2. Disclosure to Law Enforcement

The proposed solution allows Wisconsin (and other states utilizing the HIPAA standard) to adopt a national standard for access to protected health information by law enforcement, providing consistency in approach and implementation of law enforcement access. The solution also continues to protect patient privacy by allowing access without consent only when society's need to know overrides the patient's right of privacy. Exchanges between states would be simplified if each state adopted the national standard.

Standardization of access by law enforcement would decrease variation in deciding which of and how the varying controlling laws are applied. Administrative and cost savings would result from a standardized approach to requests for health information by law enforcement. With a standard approach, business processes would be streamlined and education and training costs would decrease.

3. Re-disclosure

The current statute prevents open exchange of information and creates segregated pockets of information rather than unified, consolidated patient information. This solution eliminates a barrier to information exchange created by a strict prohibition on re-disclosure of PHI received without patient consent under Wisconsin Statutes section 146.82(b). This solution also eliminates the need to identify the source of specific elements of a patient's record prior to disclosing PHI, thereby reducing the complexity of the disclosure process. It will also eliminate variations in practice caused by variations in interpretation of the legal requirements.

This solution offers a number of other benefits to health care providers and recipients: it increases provider access to patient information for treatment purposes, decreases the chances of an erroneous disclosure, and increases consistency of information disclosed. In addition, by simplifying the Wisconsin law, this solution will increase compliance, control costs, and improve patient safety.

4. Documentation

By eliminating the statutory requirement to document disclosures of health information, the barriers caused by these regulations are removed. This would create significant reductions in burdensome

documentation and administrative cost to implement and monitor documentation. This would also result in significant cost savings as employees would no longer need to determine which law applies and the elements required to be documented, then document the elements required for the release of information. Training costs would be greatly reduced as well. This cost savings could potentially be passed along to patients.

Removing the documentation requirements would not reduce patient privacy. There are very few cases in which a patient requests to view access by others to his/her records and for the very few who do, many Workgroup members indicated that the current requirements are burdensome and costly.

There is concern that current IT systems do not have the capability to collect the necessary elements for documentation. Under current state law, those organizations that rely on audit trails created by their IT systems for documentation could be liable for not documenting the required elements, as could their vendors.

TYPES OF HEALTH INFORMATION EXCHANGE ADDRESSED: Amend Wisconsin Statutes Chapter 146

1. **Expansion of disclosure to family:** All types of health care information would be affected by this change. Examples of exchanges affected include: appointment scheduling, medications, patient health care services, immunizations and other clinical information, laboratory reports, etc. exchanged by a provider and family caretaker through phone calls, face-to face exchanges or the provision of copies of patient information.

2. **Expansion of disclosure to law enforcement:** Information from all types of health care providers to law enforcement in all health care environments would be affected by this change. Although many of these exchanges typically occur in emergency departments, the law should clearly state how to handle all requests by law enforcement for health information (i.e., by phone or in writing, in addition to in person).

3. **Removal of re-disclosure requirement:** This change affects the exchange of all PHI that is received without patient consent under Wisconsin Statutes section 146.82.

4. **Modification of documentation requirements:** Current documentation requirements (Wisconsin law and Federal Privacy Rules) apply to all disclosures of health information (not internal uses of information). Therefore all disclosures of health information would be affected by a change in the regulations.

STAKEHOLDERS AFFECTED AND INVOLVED: Amend Wisconsin Statutes Chapter 146

The grid below indicates the stakeholder groups identified by RTI that have a role in the development of, or are affected by, this proposed solution:

	Stakeholder Group																
	Clinicians	Physician groups	Federal health facilities	Hospitals	Payers	Public health agencies	Community clinics and health centers	Laboratories	Pharmacies	Long-term care facilities and nursing homes	Home Ccare and hospice	Correctional facilities	Professional associations and societies	Medical/public health schools that conduct research	Quality improvement organizations	Patients, Consumers, Advocacy Organizations	State government
1. Disclosure to Family																	
Affected by Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2. Disclosure to Law Enforcement																	
Affected by Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3. Re-disclosure																	
Affected by Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4. Documentation																	
Affected by Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Employers will also be affected by this solution. As well, legislators, vendors, and standards generating organizations (e.g., CCHIT, HITSP) will be critical partners in the development and implementation of this solution.

STAGE OF DEVELOPMENT: Amend Wisconsin Statutes Chapter 146

None of the proposed changes to Wisconsin Statutes chapter 146 have been initiated. However, the Workgroup's examination of current processes suggests that Wisconsin's requirements are not being met by many health care providers. Therefore, many of the solutions are in fact business practices currently followed today, contrary to existing law.

EXTENT SOLUTION IS IN USE: Amend Wisconsin Statutes Chapter 146

None of the proposed changes to Wisconsin Statutes chapter 146 have been initiated. However, the Workgroup's examination of business practices suggests that many providers are using the proposed solutions rather than complying with Wisconsin's (more restrictive) legal requirements.

SCALABILITY: Amend Wisconsin Statutes Chapter 146

The changes to Wisconsin Statutes chapter 146 apply to all organizations and individuals who exchange protected health information (PHI) in Wisconsin. The overriding concept of the solution is to change

state law to mirror HIPAA to allow for better exchange of information both within Wisconsin and across state boundaries. That concept can, and should, be applied across states to facilitate HIE.

POSSIBLE BARRIERS: Amend Wisconsin Statutes Chapter 146

This solution removes a perceived privacy protection provided by Wisconsin Statutes chapter 146. As with any legislative change, the process to change the law will be a barrier. There also may be lobbying groups who lobbied to create the law in the first place who will have to be persuaded.

DOMAINS ADDRESSED: Amend Wisconsin Statutes Chapter 146

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
8 - State law restrictions
9 - Information use and disclosure policy

6.2.b Modify Wisconsin Statutes section 51.30 in relation to access for treatment

The second proposed solution that falls under the category of 'solutions to issues derived from state privacy and security laws/regulations is: 'Modify Wisconsin Statutes section 51.30 in relation to access for treatment.'

CONTEXT FOR PROPOSED SOLUTION: Amend Wisconsin Statutes Section 51.30

Wisconsin Statutes governing disclosure of personal health information to providers for treatment purposes vary by the type of health information disclosed. General health information and HIV test results can be released to providers for treatment purposes without patient consent.[138] Information regarding mental health, alcohol or drug abuse, and developmental disabilities can be released under Wisconsin Statutes section 51.30 only with a patient's written informed consent except in a medical emergency or for medications, allergies and diagnosis to health care providers within a related health care entity.[139] By requiring patient consent to release information regarding mental health, alcohol and other drug abuse (AODA) and developmental disabilities, Wisconsin Statutes differ from federal HIPAA regulations, which allow release of information between providers for treatment purposes without patient consent.[140] Like Wisconsin Statutes section 51.30, the federal law that controls AODA treatment records requires patient consent to provide this information to a provider for treatment purposes.[141]

The lack of uniformity between Wisconsin Statutes section 51.30 and other state and federal privacy regulations present a number of barriers to the disclosure of health information to providers for treatment purposes in both paper and electronic environments. Most notably:

[138] Wisconsin Statutes section 146.82(2)(a)2.; Wisconsin Statutes section 252.15(5)(a)2
[139] Wisconsin Statutes section 51.30(4)(a)8
[140] 45 CFR 164.506
[141] 42 CFR Part 2

- Before treatment information may be shared, there must be a determination of which state privacy law applies and a determination of whether consent is required.

- Before the treatment information exchange can occur, there must be a determination of whether HIPAA applies and then whether state or federal law controls and whether consent is required.

- Before the treatment information exchange can occur, there must be a determination of whether the federal AODA law applies and whether consent is required.

- Before treatment information can be exchanged, a valid consent with the required elements and the appropriate signature must be obtained.

PROPOSED SOLUTION: Amend Wisconsin Statutes Section 51.30

The Workgroup advocates changing Wisconsin Statutes section 51.30 clauses governing information access for treatment purposes to be consistent with the language in HIPAA. This proposed solution would allow the exchange of all personal health care information, with the exception of psychotherapy notes as defined by HIPAA and AODA treatment information governed by 42 CFR Part 2, between providers for treatment purposes without patient consent.[142]

The Workgroup discussed a number of additional areas where adjusting Wisconsin Statutes section 51.30 to match HIPAA could positively affect health information exchange, and recommends further consideration of modification of the following areas of the statute: disclosure to family; disclosure to law enforcement; and documentation requirements.

SOLUTION DESCRIPTION: Amend Wisconsin Statutes Section 51.30

Wisconsin Statutes section 51.30 should be changed to be consistent with HIPAA, such that all treatment records are disclosed to providers for treatment purposes without patient consent, with the exception of psychotherapy notes as defined by HIPAA. Moreover, HIPAA should become the national standard for disclosures/exchanges between providers for treatment purposes, making all such exchanges allowable without patient consent in all states. This change would enable all states to utilize the HIPAA definitions and requirements, creating uniform definitions of 'treatment,' 'consent,' and 'health care provider.'

BARRIERS ADDRESSED: Amend Wisconsin Statutes Section 51.30

This solution eliminates variation in Wisconsin law by removing the requirement to secure patient consent to release certain types of health information to providers for treatment purposes. It also eliminates variation between Wisconsin law and the HIPAA privacy law. (It does not address the variation between the federal AODA law, 42 CFR Part 2, and HIPAA.)

[142] This proposed solution was adjusted by the Implementation Workgroup to initiate an inclusive process to identify specific changes to 51.30 that all impacted stakeholders can support.

This solution provides a number of added benefits for providers and patients. Consistency in the regulations governing health information disclosure and consent will remove barriers to health information exchange, eliminating treatment delays due to unavailable or incomplete information and associated risks to patient safety, and thereby improving the quality of patient care. Moreover, clearer definitions of 'treatment,' 'health care,' and 'provider' will reduce ambiguities in release practices, leading to more efficiency in the exchange of health care information. The Workgroup believes that these changes will lead to dramatic improvements in patient care, decreases in costs for providers and patients, and improvements in providers' ability to share patient information across states.

TYPES OF HEALTH INFORMATION EXCHANGE ADDRESSED: Amend Wisconsin Statutes Section 51.30

This solution affects all exchanges of all health information currently regulated by Wisconsin Statutes section 51.30 among providers for treatment purposes.

STAKEHOLDERS AFFECTED AND INVOLVED: Amend Wisconsin Statutes Section 51.30

The grid below indicates the stakeholder groups identified by RTI that have a role in the development of, or are affected by, this proposed solution:

	Stakeholder Group																
	Clinicians	Physician groups	Federal health facilities	Hospitals	Payers	Public health agencies	Community clinics and health centers	Laboratories	Pharmacies	Long-term care facilities and nursing homes	Home Care and hospice	Correctional facilities	Professional associations and societies	Medical/public health schools that conduct research	Quality improvement organizations	Patients, Consumers, Advocacy Organizations	State government
Affected by Solution	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X

STAGE OF DEVELOPMENT: Amend Wisconsin Statutes Section 51.30

Wisconsin laws regulating general health and HIV record release for treatment do not require patient consent for exchange and are consistent with HIPAA. One of the state's networked organizations also uses the HIPAA standard that allows disclosure without consent. These processes have worked well in Wisconsin and provide a possible template to handle mental health and developmental disability records as proposed by this solution. (Note: Release of AODA treatment records will still require patient consent per 42 CFR Part 2.)

The Workgroup noted a number of steps towards implementing this solution, including gaining the support of appropriate professional associations and consumer organizations, by finding common ground with advocates; drafting model legislation; working toward legislative changes; and providing provider and consumer education.

EXTENT SOLUTION IS IN USE: Amend Wisconsin Statutes Section 51.30

As noted above, this solution already governs the release of general health and HIV records in Wisconsin. In addition, one networked organization in Wisconsin also uses the HIPAA standard that allows disclosure of mental health and developmental disability information for treatment purposes without consent.

SCALABILITY: Amend Wisconsin Statutes Section 51.30

This solution reduces barriers to health information exchange, and should be feasible for organizations of all types and sizes. Changing Wisconsin law Wisconsin Statutes section 51.30 to mirror HIPAA for exchange, between providers for treatment would simplify the process for providing patient care across state lines.

POSSIBLE BARRIERS: Amend Wisconsin Statutes Section 51.30

This solution removes a privacy protection provided by Wisconsin Statutes section 51.30. There are very strong groups in Wisconsin who fought to create this legislation, making it difficult to removing these privacy protections at the state level. Thus, involving a broad variety of consumers, patients, providers, and health care advocates in the decision-making and implementation process will be critical to bring this solution to the implementation phase. Recent modifications to Wisconsin Statutes section 51.30 have allowed expanded access to patient health care information by providers within a related health care entity, so this may be an opportune time to consider discussing further modification to this law.

State laws with more stringent protection than HIPAA, such as Wisconsin Statutes section 51.30, would hinder the intrastate exchange of health information for treatment purposes. Thus, additional research should be done to determine which other states have laws that are more restrictive than HIPAA regarding the disclosure of health information to providers for treatment purposes.

As Wisconsin transitions to an electronic environment, additional consideration should be given to the regulations governing information 'access' as opposed to 'disclosure.' These efforts should examine what is disclosed to whom under which circumstances, with serious consideration given to the establishment of uniform access controls within Wisconsin and between states.

DOMAINS ADDRESSED: Amend Wisconsin Statutes Section 51.30

1 - User and entity authentication
2 - Information authorization and access controls
8 - Laws
9 - Information use and disclosure policy

ALTERNATIVE SOLUTION: Amend Wisconsin Statutes Section 51.30

In the event that this solution is not feasible, an alternate solution was proposed. This alternate solution would expand on the recent changes to Wisconsin Statutes section 51.30, such that the data elements outlined under Wisconsin Statutes section 51.30(4)(b)8g could be exchanged for treatment purposes without consent by health care providers that are not part of the same network.

6.3 Solutions to issues driven by intersection between federal and state laws/regulations

'Solutions to issues driven by intersection between federal and state laws/regulations' is the third major solution category outlined by RTI. This category includes four sub-categories:

- Solutions applicable to general privacy/security federal laws and regulations (e.g., HIPAA Privacy, HIPAA Security);
- Solutions applicable to state programs (e.g., Medicaid);
- Solutions that would address issues of non-compliance with federal laws/regulations (such as non-compliance with HIPAA Privacy, HIPAA Security); and
- Education solutions to address misinterpretations of federal laws/regulations.

One solution proposed by the Workgroup falls under the category of solutions to issues driven by the intersection between federal and state laws/regulations: propose changes to HIPAA. This solution also falls under the category of national-level recommendations and, therefore, is only summarized below. A more detailed discussion of this solution is provided in Section 7 of this report.

As indicated in the matrix below, this multi-component solution addresses multiple sub-categories defined by RTI. Each component of the solution applies to HIPAA. Two components, *eliminate BAAs* and *clarify the "minimum necessary" requirement*, also address issues of non-compliance identified through this project's Variations and Legal workgroups discussions and include education to address misinterpretation issues.

Section 6.3, Table 4. Solutions to issues driven by intersection between federal and state laws/regulations

Solution	Solution Sub-categories Defined by RTI			
	Applies to HIPAA	**Applies to State Programs**	**Address Non-compliance with Federal Law**	**Education to Address Misinterpretation Issues**
Change HIPAA				
Eliminate BAAs	X	X	X	X
Remove Research Waiver Req.	X			
Clarify "Minimum Necessary"	X		X	X

CONTEXT FOR PROPOSED SOLUTION: Propose Changes to HIPAA

The HIPAA Privacy Rule introduced a number of requirements intended to protect patient privacy. In some instances, however, the Workgroup feels that HIPAA's requirements increased administrative burdens that impede health information exchange while providing only nominal improvements in patient privacy protections. In other instances, HIPAA's requirements provide important protections to patient privacy but are broadly interpreted and implemented with wide variation. In relation to both of these instances, the Workgroup recommends revising HIPAA.

PROPOSED SOLUTION: Propose Changes to HIPAA

The Workgroup advocates proposing changing the language of the Federal Privacy Rule, HIPAA, in three areas:

1. **Business Associate Agreements (BAA):** Remove the requirement to have a BAA, but hold business associates accountable for adhering to state and federal privacy requirements and liable for privacy violations under state and federal statutes.

2. **Research:** Remove the waiver process required to proceed for research without patient consent, but maintain Institutional Review Board (IRB) process requirements.

3. **"Minimum necessary":** Develop model policies and procedures to clarify the "minimum necessary" standard.

A more detailed discussion of this solution is provided in Section 7 of this report.

6.4 Solutions to enable interstate e-health information exchanges

'Solutions to enable interstate eHealth information exchanges' is the fourth major solution category outlined by RTI. Whereas the first three solution categories reflect responses to the barriers identified through this project's Legal and Variations workgroups, this final category reflects a key project goal: supporting health information exchange. The Solution Workgroup's belief that any inconsistencies between Wisconsin and federal law as well as variations in business practices and policies will impede health information exchange was a driving factor in the development of each solution presented in this report. Thus, as indicated in the matrix below, each of the solutions proposed by the Workgroup could be placed under the category of 'solutions to enable interstate e-health information exchanges.'

Section 6.4, Table 5. Solutions affecting interstate health information exchange

Solution	
Change Wisconsin Statutes chapter 146	X
Change HIPAA	X
Change Wisconsin Statutes section 51.30 (sensitive information)	X
Standardize Verification of Patient	X

Each solution is profiled in more detail in its primary category.

Section 7 – National-level Recommendations

7.1 Introduction

When reviewing barriers identified by the Variations and Legal workgroups, it became clear that while the HIPAA Privacy and Security Rules create many necessary patient privacy protections, some of the language in HIPAA presents barriers to the exchange of health information that either do not improve patient privacy protections enough to merit the burden of the requirement or allow for broad interpretation which leads to wide variation in business practices.

The Solutions Workgroup reviewed each barrier to health information exchange that HIPAA imposes, as identified through the scenarios from the Variations and Legal workgroups, then decided which barriers

should remain and which should be reduced or eliminated. The Workgroup then developed a solution that proposes changes to HIPAA to address the barriers that need to be reduced or eliminated.

The proposed changes to HIPAA are detailed in the following section. Because HIPAA is a national law and this solution must be implemented at the national level, this solution is presented in this section, which presents national-level solutions recommended by Wisconsin's Solutions Workgroup.

The Final Implementation Report will not address these proposed changes to HIPAA. The Implementation Workgroup felt it would be a better for the implementation plan for this solution to be created at the national level by individuals experienced with national-level legislative change.

7.2 Propose changes to HIPAA

After reviewing all barriers associated with HIPAA that were identified by the Variations and Legal workgroups, the Solutions Workgroup proposed revisions in the following three areas:

1. Business associate agreements
2. Research requirements
3. "Minimum necessary"

PROPOSED SOLUTION

The Workgroup advocates proposing changes to the language of the Federal Privacy Rule, HIPAA, in three areas:

1. **Business Associate Agreements (BAA):** Remove the requirement to have a BAA, but hold business associates accountable for adhering to state and federal privacy requirements and liable for privacy violations under the law.

2. **Research:** Remove the waiver process required to proceed with research without patient consent, but maintain Institutional Review Board (IRB) process requirements.

3. **"Minimum necessary":** Develop model policies and procedures to clarify the "minimum necessary" standard.

SOLUTION DESCRIPTION

The section that follows presents each element of this three-part solution in detail, summarizing the topic area in Wisconsin today as well as the proposed solution.

Business Associate Agreements

Prior to HIPAA, when confidential information was exchanged, there was typically 'confidentiality language' in contracts regarding the protection and use of confidential information in services performed. Wisconsin recognized most of these relationships as legal contractual relationships, agency relationships,

or employment agreements and applied required privacy protections to those individuals or groups using protected health information to perform services on behalf of health care providers.

HIPAA formalized the contractual language with a mandate for Business Associate Agreements (BAAs) between covered entities and the inclusion of specific privacy protection language. This mandate stemmed in part from the HIPAA Privacy Rule's omission of a mechanism that provides accountability for individuals accessing protected health information when performing services for covered entities. The HIPAA BAA requirement provides accountability for activities of the business associate through the covered entity[143] and the contractual arrangement of the BAA.

HIPAA requires that whenever a covered entity is supplying information directly or indirectly to an outside person or entity and that information includes protected health information (PHI), the covered entity must consider whether a business associate relationship is being created and whether a BAA is necessary.[144] There is no requirement for this type of contractual agreement under Wisconsin law. However, within Wisconsin laws and codes, there are requirements to contractually protect confidential information in certain circumstances.[145]

Determining whether a BAA is needed is an administratively burdensome process. Drafting BAAs is similarly time- and resource-intensive: separate, unique BAAs are required for almost every business associate. Although there is a national standard for BAA language, it is not uniformly applied. BAAs can also be confused with trading partner agreements. On balance, Workgroup members consider BAAs to be burdensome and costly undertakings with little gain to operational efficiency or patient privacy. **Thus, the Workgroup recommends eliminating HIPAA's requirement to have a BAA, and creating a mechanism to hold business associates accountable under state and federal statute in case of breach, state privacy, or HIPAA violation.**

Research

In Wisconsin, prior to HIPAA, access to research information without patient consent was controlled by the statutory exceptions in the state privacy laws.[146] HIPAA's requirements governing access for research

[143] Covered entities include health plans, health care providers, and clearinghouses.

[144] A business associate is a person or company who performs or assists in the performance of a function or activity on behalf of a covered entity (health care provider) involving the use or disclosure of protected health information (PHI). In addition, if any person or company in the following categories is hired by a covered entity and PHI is disclosed to them as part of their agreement with the covered entity, they are a business associate: legal, actuarial, accounting, consulting, certain data aggregation services, management, administrative, accreditation, or financial services. Business associates perform a range of functions and activities, including: claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, and practice management.

[145] For example, for the purposes of Medicaid administration, the state is required to have some type of agreement unless there is a legal requirement to provide the data. For more, see: HFS 108.01 (5) – HFS 108.01(6)(b).

[146] Wisconsin statutes generally allowed access if the researcher was affiliated with the health care provider and provided written assurances that the information would be used only for the purpose requested and no identifiable information would be disclosed in the final research product. In addition, Wisconsin Statutes section 51.30, controlling more sensitive information, required that the research project be approved by the Department of Health and Family Services, and Wisconsin Statutes section 252.15, regulating HIV test results, required that the project be approved by an Institutional Review Board (IRB). In addition, although this is not required by the privacy laws, research studies involving human subjects were approved by an IRB. If a researcher did not meet these requirements, patient consent for research access would be required. For additional information, see Wisconsin Statutes section 146.82(2)(a)6, 51.30(4), 252.15(5)10.

purposes are deemed more protective of patient information than state laws and, therefore, the HIPAA requirements control access without consent for research purposes. Under HIPAA, if researchers request access to identifiable health information as part of a research study, they must either obtain a waiver from the Institutional Review Board (IRB) as part of the IRB approval process or obtain consent from all patients in the study.[147] Due to the additional waiver criteria required by HIPAA, many facilities have created privacy boards in addition to the IRB to evaluate and grant waivers.

In evaluating a research proposal, an IRB is required to weigh the proposal's risks and benefits, including its impact on the confidentiality of patient health information. It is the Workgroup's consensus that IRB approval is sufficient to protect patient confidentiality. **Thus, the Workgroup proposes eliminating 45 CFR 164.512(i)(2)(ii), the clause in HIPAA that specifically requires the additional waiver criteria.**

Minimum Necessary

The "minimum necessary" standard, a specific protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today.[148] It is based on sound current practice that the disclosure of protected health information should be limited to that which is necessary to satisfy a particular purpose or carry out a function. The "minimum necessary" standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's "minimum necessary" requirements are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.[149]

The Privacy Rule requires that the "minimum necessary" standard be applied unless the regulations specifically state that the standard is not required to be applied. Application of the standard is distinctly different for uses other than disclosures; the standard is also applied differently for routine and non-routine disclosures. The Privacy Rule generally refers to uses as internal sharing of information, and disclosures as release of information outside the facility or system. The Privacy Rule is written such that each covered entity interprets the "minimum necessary" standard in its own policies and procedures.

Application of the "minimum necessary" standard creates a significant barrier to health information exchange. The standard makes it difficult to determine what is to be disclosed and allows for subjective decision-making on the amount of information that is disclosed. Moreover, it makes it difficult to know what information will be received.

The Workgroup noted that it may not be feasible to adhere to the "minimum necessary" standard in many electronic health information systems. In an electronic exchange, "minimum necessary" may require limitation of access or other technology that allows for layered access. In organizations with paper records, for exchanges subject to the "minimum necessary" standard, an individual must sort through the chart and copy only the relevant pieces of information before releasing the information. The standard therefore may require specific technology requirements and/or specially trained staff to evaluate records, which may increase the costs and administrative burden of the disclosure process.

In addition to the requirements of the law, variation in business practice as a result of varying interpretations of the loosely defined law creates further barriers to information exchange. If one organization limits information in one way while the organization it is exchanging with limits it another

[147] 45 CFR 164.512(i)(2)(ii)
[148] 45 CFR 164.502(b), 164.514(d)
[149] OCR HIPAA Privacy, December 3, 2002, Revised April 4, 2003

way, for example, it is difficult to obtain the information required for the intended purpose. The inconsistency in the standard may also result in insufficient information being provided when necessary for patient health care processes.

Thus, the Workgroup recommends both re-writing the applicable section of Wisconsin Administrative Code 92.03(1)(n) that pertains to "minimum necessary" so that it mirrors HIPAA, and developing state and national model policies and procedures for defining and applying the "minimum necessary" standard.

BARRIERS ADDRESSED

Business Associate Agreements

Removing the requirement to have a BAA eliminates the need to dedicate resources to determining when a BAA is necessary and, when necessary, drafting and monitoring BAAs. This solution simplifies the process for exchanging information. Moreover, it enables covered entities to redirect resources currently allocated to BAAs to benefit health care operations and patient care. This should reduce costs for everyone involved, possibly contributing to a reduction in health care costs. Once federal law is changed, this solution would be inexpensive to implement and would have nominal impact on patient privacy.

Research

Maintaining the IRB process but removing the waiver process required to proceed without patient consent eliminates a barrier to health information exchange for research purposes, thereby enhancing and encouraging research projects that are IRB approved. While the legal solution proposed still maintains the patient privacy protections provided by the IRB, it reduces the administrative costs of conducting research by removing the additional and often redundant step of applying for, reviewing, and ultimately granting waivers to access health information for research purposes.

Minimum Necessary

This solution does not recommend removal of the barrier imposed by the "minimum necessary" standard because the Workgroup believes the standard is necessary for patient privacy protection. The Workgroup maintains that information released should be limited to what is required to meet the intended purpose. Instead, this solution addresses the variability in application of the "minimum necessary" standard with a request for development of model policies and procedures to clarify the standard.

Clarifying and standardizing the "minimum necessary" requirement has many benefits. First and foremost, it simplifies and streamlines the exchange of information. In addition, it helps guarantee that organizations receive the information they need to meet the purpose of the exchange. Clear standards also reduce the amount of time required to fulfill a request for information as it will be easier to ascertain what information should be released. Finally, with a simplified process, it will become easier and less resource-intensive to train staff on the "minimum necessary" standard. If the standards are adopted nationally, this will benefit exchanges between all types of organizations, at the state, regional, and national level.

TYPES OF HEALTH INFORMATION EXCHANGE ADDRESSED

Business Associate Agreements: All exchanges of health information between organizations and individuals that meet the current definition of covered entity and business associate.

Research: All types of health care research and those involved in these processes, including patients, health care facilities, researchers, health care providers, public health, quality assurance programs and developers of drugs and treatment programs that use patient health care information in their research.

"Minimum necessary": All exchanges of health care information that are covered by HIPAA will be affected by this proposed change to HIPAA. Furthermore in Wisconsin, all exchanges of information covered by Wisconsin Statutes section 51.30 (mental health, alcohol and other drug abuse and developmental disability information) would be affected.

STAKEHOLDERS AFFECTED AND INVOLVED

The grid below indicates the stakeholder groups identified by RTI that have a role in the development of, or are affected by, this proposed solution:

	Stakeholder Group																
	Clinicians	Physician groups	Federal health facilities	Hospitals	Payers	Public health agencies	Community clinics and health centers	Laboratories	Pharmacies	Long-term care facilities and nursing homes	Home Care and hospice	Correctional facilities	Professional associations and societies	Medical/public health schools that conduct research	Quality improvement organizations	Patients, Consumers, Advocacy Organizations	State government
Business Associate Agreements																	
Affected by Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Research																	
Affected by Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
"Minimum Necessary"																	
Affected by Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Involved in Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

STAGE OF DEVELOPMENT

Business Associate Agreements: Any health care provider that is required to comply with HIPAA is already using this solution. As there is no BAA requirement under Wisconsin law, this solution was also use throughout the state before the introduction of HIPAA.

Research: Before HIPAA, the IRB process was used effectively to protect patient confidentiality in Wisconsin. There were no documented breaches of patient privacy related to research in court proceedings. A return to pre-HIPAA requirements would be a relatively easy transition in Wisconsin.

"Minimum necessary": This solution has not been implemented anywhere. The Workgroup is not aware of any initiatives under way to implement it.

EXTENT SOLUTION IS IN USE

This solution is not currently in use.

POSSIBLE BARRIERS

It is a long and arduous process to change federal law. Thus, it could take years to achieve this solution.

In addition, simplifying the process for providing access without consent for research under federal law may not eliminate more restrictive state laws in other states that would preempt federal law. The national elimination of the waiver requirement may still result in a state-by-state patchwork of variable legal requirements relating to access for research purposes. States that have more restrictive privacy requirements than the proposed IRB-approval-only process would continue to have difficulty exchanging information for research purposes.

DOMAINS ADDRESSED

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

ALTERNATIVE SOLUTION

Research

Understanding that a change in federal law may be difficult to achieve in a timely manner, another solution might be to obtain a specific type of consent from a patient that would allow access for research that would be ongoing throughout the provision of health care services. This solution could be enhanced by the design of a standardized, nationally-accepted consent form allowing for very broad access and use of health care information for research purposes.

Section 8 – Conclusions and Next Steps

The eHealth Board extends its sincere appreciation to all of the volunteers who dedicated their time to the Security and Privacy Project. The information that has been collected through this process will be valuable as the eHealth Board begins the implementation phase in developing electronic systems and a means to exchange health information electronically.

The recommendations contained in the report represent possible solutions to the challenges identified through the analysis of the 18 scenarios. The recommendations are intended to inform policy discussions, but should not be construed as comprehensive or definitive legislative recommendations of the eHealth Board at this time. The eHealth Board will be using the Security and Privacy Project reports to assess where the proposed solutions fit within the eHealth Board's scope of work for the coming years. Wisconsin is committed to developing the necessary policies and procedures to ensure the adoption of health information technology and exchange throughout Wisconsin in an effort to ensure quality of care and patient safety.

Appendices

Appendix 1: Variations Workgroup Members

Wisconsin
Security and Privacy Project

Variations Workgroup

Chair: **Chrisann Lemery**, WEA Trust Insurance

Paul Baum, Group Health Cooperative

Beth DeLair, UW Health, Hospital and Clinics

Jane Ducker, UW Health, Hospital and Clinics

John Hartman, representing the Wisconsin Medical Society

Jay Gold, MetaStar, Inc.

Daniel Hopfensberger, Division of Public Health, DHFS

Lowell Keppel, Wisconsin Academy of Family Physicians (WAFP)

Janice Krall, Mendota Mental Health Institute

Kathy Lindgren, ACL Laboratories

Gloria Marquardt, Department of Corrections

Lori McDonald, Wm. S. Middleton Memorial Veterans Hospital

Teresa Smithrud, Mercy Health System

Victoria Wolf, Wisconsin Lutheran Child and Family Services

Sheila Zweifel, University of Wisconsin, Health Services

Appendix 2: Legal Workgroup Members

Wisconsin
Security and Privacy Project

Legal Workgroup

Chair: **Chrisann Lemery**, WEA Trust Insurance

Cheryl Becker

Sue Bevsek

Mary Burke, Wisconsin Office of the Attorney General

Sarah Coyne, Quarles and Brady

Beth DeLair, UW Health, Hospital and Clinics

Jay Gold, MetaStar

Kathy Johnson, Department of Health and Family Services

Elizabeth Malchetske, Appleton Medical Center

Susan Manning, Privacy Consultant

Kerry Taylor, St. Vincent's Hospital

Ralph Topinka, Mercy Health Center

Nancy Vogt, Aurora Health Center

Carol Weishar, Milwaukee Medical Center

Appendix 3: Solutions Workgroup Members

Wisconsin
Security and Privacy Project

Solutions Workgroup

Members

Chair: **Jay Gold**, MetaStar, Inc.

Paul Baum, Group Health Cooperative

Tom Berg, Marshfield Clinic

Becky Borchert, Hospice, Inc.

Sarah Coyne, Quarles and Brady

Beth DeLair, UW Health, Hospital and Clinics

Mary Gulbrandsen, Madison Metropolitan School District

Stephanie Harrison, Wisconsin Primary Health Care Association

John Hartman, Visonex Corporation

Peggy Hintzman, Wisconsin State Laboratory of Hygiene

Kathy Johnson, Department of Health and Family Services

Lowell Keppel, Wisconsin Academy of Family Physicians (WAFP)

Laura Leitch, Wisconsin Hospital Association

Chrisann Lemery, WEA Trust

Thomas Luetzow, representing the Wisconsin Medical Society

Elizabeth Malchetske, Appleton Medical Center

Susan Manning, Privacy Consultant

Gloria Marquardt, Department of Corrections

Lori McDonald, Wm. S. Middleton Memorial Veterans Hospital

Thomas Moore, Wisconsin Health Care Association

Alice O'Connor, Murphy Desmond, S.C.

Barbara Oswald, Wisconsin Office of the Attorney General

Patty Pate, PIC Wisconsin

John Sauer, Wisconsin Association of Homes and Services for the Aging

Thomas Shorter, Godfrey and Lahn, S.C., Attorneys at Law

Theresa Smithrud, Mercy Health System

Susan Turney, Wisconsin Medical Society

Jane Wegenke, U.W. School of Medicine and Public Health, Comprehensive Cancer Center

Carol Weishar, Milwaukee Medical Clinic

Hugh Zettel, GE Healthcare

Sheila Zweifel, U.W. - Madison University of Health Services

Appendix 4: Security and Privacy Project Team

Wisconsin
Security and Privacy Project Team

Alison Bergum, Population Health Institute, University of Wisconsin School of Medicine and Public Health

Stacia Jankowski, Division of Health Care Financing, Department of Health and Family Services

Kathy Johnson, Office of Legal Counsel, Department of Health and Family Services

Susan Manning, Privacy Consultant

Audrey Nohel, Bureau of Health Information and Policy, Division of Public Health, Department of Health and Family Services

Judith Nugent, Bureau of Health Information and Policy, Division of Public Health, Department of Health and Family Services

Jill Piasecki, Population Health Institute, University of Wisconsin School of Medicine and Public Health

Marie Whitsell, Office of Strategic Finance, Department of Health and Family Services