

Section 9: Legal and Policy

The Wisconsin Statewide Health Information Network (WISHIN) is leading the way to enable Health Information Exchange (HIE) in Wisconsin. As the state designated entity for HIE, WISHIN is working to create a network of networks that will give health care providers a secure system to access medical information where they need it – when they need it.

9 Legal and Policy

The WIRED for Health Board established a legal and privacy framework intended to optimize and enable the electronic exchange of health information. The two principal areas of the legal and privacy framework are:

- 1) Security & Privacy Mechanisms
- 2) Mechanisms for Participation, Oversight, and Accountability

The legal and privacy framework developed by the WIRED for Health Board is the same structure used to govern the WISHIN Policy Advisory Committee and Policy Workgroups.

9.1 Privacy and Security Strategy

9.1.1 Analysis of Privacy and Security Issues Related to HIE

Wisconsin has conducted significant analysis of privacy and security issues affecting in-state and out-of-state disclosures of electronic health information using health information exchange. This analysis was completed as part of Wisconsin's participation in the Health Information Security and Privacy Collaboration (HISPC) project, the work of the eHealth Board, a Section 51.30 (Mental Health/Substance Abuse) Work Group specially convened by the DHS in 2007, and the WIRED for Health Board. A full summary of completed analyses can be found in [Appendix #](#).

9.1.2 Key Differences between Wisconsin and Federal Law

Wisconsin, like many other states, has state laws that provide heightened consent requirements for the disclosure of certain types of health information. Wisconsin statutes and rules impose specific consent requirements with respect to certain disclosures of certain health information related to mental health, developmental disabilities, and HIV/AIDS test results made for the purposes of treatment, payment, and health care operations. These requirements are more stringent than HIPAA which would not require consent for disclosures of such information for treatment, payment, and health care operations purposes.

Further analysis of key differences between Wisconsin and Federal Law can be found in [Appendix #](#).

9.2 Legal and Policy Framework

9.2.1 Developing the Legal and Policy Framework

Wisconsin's legal and policy framework for health information exchange was established based on the following near-term goals and objectives:

- 1) Establish a policy framework that optimizes the electronic exchange of health information while protecting patient privacy.
 - a) Establish uniform privacy and security strategies, policies, and procedures for the statewide health information network and HIE services that ensure health information is protected in accordance with Wisconsin law, HIPAA, and other federal laws and requirements (i.e., consent, authorization, authentication, access, audit, breach, etc.).
 - b) Establish uniform business, technical, and operational policies, and procedures for the statewide health information network and HIE services that ensure health information is protected in accordance with Wisconsin law, HIPAA, and other federal laws and requirements.
 - c) Develop of a process for establishing strategies, policies, and procedures identified in objectives (a) and (b) above incrementally over time.
 - d) Consistent with the established legal and policy framework, establish a contractual model for governing participation in the statewide health information network and HIE services in Wisconsin and in exchange with federal agencies.
 - e) Establish oversight and accountability mechanisms that ensure compliance with the established legal and policy framework by the statewide health information network and participants.
 - f) Develop a process to evaluate and update the legal and policy framework as part of an annual program evaluation and more often if necessary consistent with Objectives (a) and (b) above.
 - g) Collaborate with neighboring states beginning with Minnesota to harmonize laws, regulations, policies, and practices in support of interstate HIE.
- 2) Establish a legal framework that enables the electronic exchange of health information while protecting patient privacy.
 - a) Recommend changes to Wisconsin health privacy laws and regulations where warranted.
 - b) Advocate for harmonization of existing federal and State laws to enable HIE services.
 - c) Consistent with the established legal and policy framework, establish a contractual model for governing participation in the statewide health information network and HIE services in Wisconsin and in exchange with federal agencies.
 - d) Establish oversight and accountability mechanisms that ensure compliance with the established legal and privacy framework by the statewide health information network and participants.

- e) Develop a process to evaluate and update the legal and policy framework as part of an annual program evaluation and more often if necessary consistent with Objectives (a) and (b) above.
- f) Collaborate with neighboring states beginning with Minnesota to harmonize laws, regulations, policies, and practices in support of interstate exchange.

Furthermore, Wisconsin's legal and policy framework includes the following long-term goals and objectives:

- 1) Evaluate and update the policy framework as part of an annual program evaluation and more often if necessary to optimize electronic exchange of health information while protecting patient privacy.
 - a) Position the statewide health information network for participation in the nationwide health information network.
- 2) Evaluate and update the legal framework as part of an annual program evaluation and more often if necessary to enable the electronic exchange of health information while protecting patient privacy.
 - a) Position the statewide health information network for participation in the nationwide health information network.

In addition to the aforementioned near-term and long-term goals and objectives, Wisconsin's legal and policy framework also takes into consideration existing Wisconsin, Federal, and other states' laws Privacy and security laws, liability laws, HITECH, contract law, health care regulation, Wisconsin's WIRED for Health Act, and other laws that impact the core legal and policy topics that WISHIN must address as it implements the SHIN.

Wisconsin identified security and privacy mechanisms and participation, oversight, and accountability mechanisms as the core legal and policy topics that must be addressed as part of its legal and policy framework. Together, these two topics have overlapping influence on the more specific policies and procedures that were created and will be finalized as part of WISHIN's Phase II implementation.

A visual summary of Wisconsin's legal and policy framework is illustrated in the following figure.

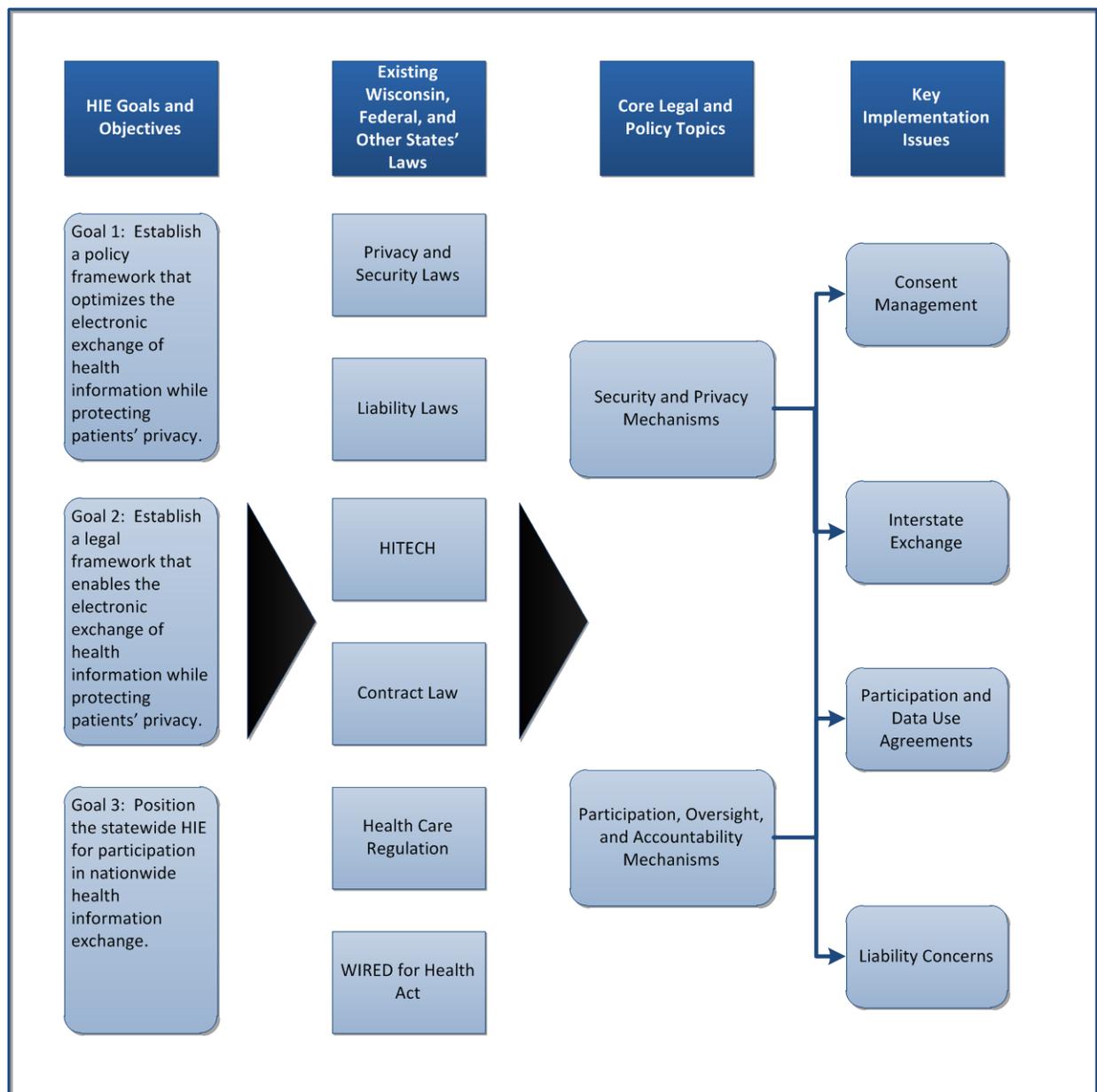


Figure 9.2.1: Legal and Policy Framework

The WISHIN Policy Advisory Committee and Policy Workgroups, comprised of Policy stakeholders, conducted analysis and provided recommendations to address the key implementation issues listed in the illustration.

9.3 Security and Privacy Mechanisms

Strong mechanisms must be in place to ensure patient information is not inappropriately used or accessed to the detriment of the patient. Inappropriate use of patient information can be deterred using a combination of security measures and privacy measures. Security measures include administrative, technical, and physical safeguards designed to prospectively protect information from being misused, such as firewalls and data encryption, or to retrospectively deter and identify misuse, such as electronic audit trails. Privacy measures include procedural standards to protect information. Some privacy procedures, such as consent requirements, are intended to prospectively protect information from being misused by limiting access to information, while other privacy procedures, such as breach notification requirements and disclosure accounting requirements, are intended to retrospectively deter and identify misuse.

Historically, Wisconsin policymakers have relied exclusively on privacy measures to prevent inappropriate use of patient information. Alternatively, through the federal HIPAA and HITECH laws and regulations, Federal policymakers have chosen to use a balance of security measures and privacy measures to protect a patient's health information.

Wisconsin's approach sufficiently served the era of paper health care records where electronic security was not possible. However, the Federal approach better serves the digital era of electronic health care records by protecting patient health information from inappropriate use through security measures and by facilitating improved patient care through privacy measures that enable more rapid communication of needed health care information. Wisconsin is pursuing updates to its medical record policies and laws that will (1) strengthen statutory mechanisms to prevent patient information from being inappropriately used and (2) facilitate improvements in patient care and reductions in patients' cost of care by encouraging health care providers to securely share patient information between patients' caregivers.

9.3.1 Consent Management

Wisconsin consent laws have been the principal legislative mechanism for preventing inappropriate use of patient information, but at the same time have been identified as a significant impediment for widespread provider participation in electronic health information exchange. For this reason, Wisconsin has spent significant time reviewing options for managing consent.

The WISHIN Policy Advisory Committee, with input from the WISHIN Technical Advisory Committee, considered WISHIN's options for designing and implementing a system of health information exchange (HIE) in the event that Wisconsin's existing mental-health privacy laws remain in place.

These laws (hereinafter referred to as “51.30”) impose state-specific consent barriers to the release of mental-health information beyond those required by the federal Health Insurance Portability and Accountability Act (HIPAA).

The Policy Advisory Committee considered the extent to which WISHIN could design its system of HIE to eliminate the 51.30 consent burden potential WISHIN clients might face as a consequence of participating in WISHIN’s Phase II query-based HIE system. These design options included:

- Suppress or filter information so that information supplied in response to a query would not include any 51.30 information, to eliminate any need to obtain 51.30 consent.
- Implement a centralized consent process to document that consent to share the information has been obtained, to eliminate any need to suppress 51.30 information.

The Policy Advisory Committee, with the guidance of the Technical Advisory Committee, concluded that while EHR systems and HIE vendors can support certain information-management and consent-management functions that would mitigate 51.30 compliance concerns, it does not appear that WISHIN could implement:

- A technological solution that could ensure that all 51.30 information could be blocked from disclosure; or
- A centralized consent management process that would address the risk-management concerns of all potential WISHIN participants.

The Committee therefore reiterated its strong preference for the enactment of HIPAA harmonization legislation in Wisconsin that would allow mental-health information to be treated in the same manner as other general health information from a privacy and consent standpoint.

In designing, procuring and implementing a statewide system of HIE, WISHIN will take steps to mitigate the privacy-compliance concerns of potential participants. However, given the complexity and vagueness of 51.30, WISHIN acknowledges that its ability to preempt any and all such concerns is limited and that potential participants will individually evaluate the risk and benefits of WISHIN participants.

WISHIN’s Phase II RFP will ask HIE vendors to explain their systems’ capabilities with respect to filtering sensitive information and managing consent centrally. WISHIN will continue to gather information about providers’ potential consent-management concerns and workflows to inform its vendor-evaluation process.

9.3.2 Interstate Exchange

The Interstate Exchange Policy Workgroup was convened to identify issues related to interstate health information exchange and discuss mitigation strategies for WISHIN.

Since interstate exchange is a well-researched and documented topic, the Workgroup leveraged materials prepared as part of the Health Information Security and Privacy Collaboration (HISPC) studies, materials available for review issued by the Upper Midwest Health Information Exchange (UM-HIE) Consortium, and researched gathered by the WIRED for Health Board.

The Workgroup identified the following Policy issues and mitigation strategies.

Priority	Identified Risk	Description	Mitigation Strategy
1	State Statutes for Consent	Numerous states, including Iowa, Minnesota, and Ohio, have consent laws that are more restrictive than HIPAA.	Wisconsin should pursue HIPAA Harmonization efforts. If legislation is not passed, Wisconsin should procure a robust consent management module and develop policies and procedures in compliance with existing state and federal statutes.
2	Exchange of Sensitive Health Information	Numerous states, including Wisconsin, Minnesota, Illinois, Michigan, and Ohio, have provisions around the transfer of sensitive health information, such as: Behavioral Health Records, HIV, Alcohol & Other Drug Abuse, Sexually Transmitted Diseases, and Genetics Testing.	Wisconsin should pursue HIPAA Harmonization efforts. If legislation is not passed, Wisconsin should implement technology that filters sensitive patient information.
3	Reciprocal Agreements between States	Providers (on the border) that see patients from other states would need to sign up for HIE services in multiple states unless coherent reciprocal agreements exist between states.	Wisconsin should support the proposed “Policy Statement Interstate Access” document discussed during the Upper Midwest Stakeholders meeting.

The Workgroup identified the following Technical risks and mitigation strategies.

Priority	Identified Risk	Description	Mitigation Strategy
1	Technology Standards	Standards, such as HL7 and IHE, do not provide enough rigor in message formats to guarantee that data conforms for interstate exchange. This means a Continuity of Care Record (CCR) or Continuity of Care Document (CCD) may not be cross-border compatible.	WISHIN should be cognizant of emerging standards approved by ONC and should create interface control protocols consistent with these standards.
2	Authentication	Interstate exchange will require authentication from the Provider that is making the query to receive patient health information. Without a common standard for secure token passing, as well as trusted identity, this is a large risk for the exchange. These types of conflicts are what sophisticated hackers will use to penetrate the system.	WISHIN should discuss the possibility of creating an interstate exchange identity management system in collaboration with other states.
3	Patient Identification	States may use different probabilistic matching algorithms to identify patients using demographic data. This could be an issue unless some Protected Health Information (PHI) is used to identify patients. The sharing of PHI for this purpose may violate consent laws in other states.	WISHIN should leverage lessons learned from existing state programs, such as Medicaid and FoodShares, to understand patient (customer) identification mechanisms currently implemented in the state. Additionally, WISHIN should be cognizant of consent laws in other states when designing its Patient Identification system.
4	Provider Directories	States will construct provider directories in different manners, such as centralized lookup repositories for provider data. Technology must be developed to share provider information across state lines and map information to the agreed format.	WISHIN should closely monitor progress made by the Standards & Interoperability (S&I) Framework Provider Directory workgroup and leverage best practices and standards to the extent practicable.

Priority	Identified Risk	Description	Mitigation Strategy
5	Quality Measures	Different quality measures, (i.e., the detail of information exchanged, service level agreements like transmission time, and atomicity of data exchanged) will be used by states to evaluate quality. The underlying data may not be compatible which could lead to different results, especially in the consolidated repository.	WISHIN should stay abreast of developments from the ONC related to data standardization.
6	Compatibility/Interoperability of Certificate Authorities for Provider Directories	No federal mandate has been made regarding certificate authority. This impacts interstate exchange as only trusted sources certified by a certificate authority can send information within the exchange.	WISHIN should work closely with ONC to define a central certificate authority, which can certify the sources that exchange data.
7	Technology Limitations	Statewide HIEs have identified that images cannot be exchanged due to internet bandwidth limitations. This implies healthcare organizations must enforce additional policies around the exchange of this information.	Edge servers should be used by WISHIN participants to introduce local caching to reduce download and bandwidth issues from the central server.

A comprehensive report from the Interstate Exchange Workgroup can be found in [Appendix #](#).

9.4 Participation, Oversight, and Accountability Mechanisms

Since statewide HIE is an emerging field, WISHIN has created Workgroups and retained legal counsel to provide advice and develop policies as needed. These policies address privacy, security, auditing, accountability, liability, and indemnification.

9.4.1 Liability Policy

The WISHIN Liability Issues Workgroup was convened to discuss liability concerns and recommend mitigation strategies. The Workgroup identified a number of liability concerns relevant to WISHIN and its participants, as well as to others who might be impacted. The Workgroup also agreed upon recommendations for WISHIN to explore to address identified liability concerns. The following is a list of concerns identified by the Workgroup:

- 1) Negligence
 - a) Inappropriate disclosure of patient data (due to theft or accident)
 - b) Errors and omissions in data entry
 - c) Professional liability could flow from exchange of inaccurate, incomplete, or untimely information
 - d) Duty to review/failure of data users to utilize available data
 - e) Improper transmission of health information
 - f) Technology malfunction resulting in erroneous data
 - g) Mismanagement: Hiring unskilled/untrained staff, failure to supervise, failure to have or implement proper policies
 - h) Identity theft (statutes may create separate cause of action besides negligence)
- 2) Products liability (WISHIN for its participants and vice versa)
- 3) Products liability (IT Vendors/Providers)
- 4) Contractual
 - a) Master data sharing agreements (MDSAs)
 - b) Business Associate Agreements
 - c) Contracts with data providers
 - d) Contracts with data users
 - e) Contracts with technology providers

The Workgroup assessed the list of liability concerns and provided recommendations that WISHIN should consider to mitigate the risks. The comprehensive report from the Liability Issues Policy Workgroup, including liability risks and recommended mitigation strategies, can be found in **Appendix #**. WISHIN will consider the Workgroup's recommendations and incorporate in Phase II under the direction of WISHIN's legal counsel.

9.4.2 Participation and Data Use Agreements

The WISHIN Direct Rapid Implementation Workgroup drafted the WISHIN Direct Participation Agreement that outlines the provisions for WISHIN customers participating in WISHIN Direct services. This workgroup also drafted the WISHIN Bridge Participation Agreement that outlines the provisions for Vendors that participate in WISHIN Bridge.

The WISHIN Direct and WISHIN Bridge Participation Agreements were reviewed by the WISHIN Policy Advisory Committee and sent to WISHIN's legal counsel for final

changes and approval. WISHIN Direct went live in August 2011 and the Participation Agreement is executed with WISHIN clients upon enrollment in WISHIN Direct. A sample WISHIN Direct Participation Agreement can be found in **Appendix #.**

This same Workgroup responsible for drafting the WISHIN Direct and WISHIN Bridge Participation Agreements will continue to assist WISHIN in the development of Participation and Data Use Agreements required as part of WISHIN's Phase II implementation plans.

9.5 Mechanisms to Refresh Legal and Policy Framework

The overall objective of the legal and policy framework is to establish clear parameters for the collection, access, use, and disclosure of personal health information by all individuals and organizations that participate in WISHIN and engage in the exchange of health information through WISHIN. In addition, patients must be provided with access to and reasonable controls over their personal health information and security safeguards and controls must be adopted. Several legal- and policy-related activities need to occur over the long-term to help promote the adoption and sustained use of HIT and HIE and keep Wisconsin's legal and policy framework robust and meaningful in the years to come.

WISHIN's Policy Committee will continue to incrementally develop and implement uniform privacy and security strategies, policies, procedures, and practices for the SHIN that ensure health information is protected in accordance with Wisconsin law, HIPAA, and other federal laws and requirements. The development and implementation of strategies, policies, procedures, and practices will continue to be prioritized beginning with those items that need to be in place in order for the SHIN to "go live." Other items are and will continue to be developed and rolled out depending on where they fit into the overall project timeline and milestones.

The Legal and Policy Framework outlined in this section will be continually evaluated and updated as part of the required annual program evaluation and more often if necessary. As a result of that process, we anticipate recommending changes to Wisconsin health laws and regulations for both intrastate and interstate HIE, advocating for the continued harmonization of existing federal and State laws to enable HIE services, and developing new and revising existing strategies, policies, procedures, and practices for the SHIN. All of this work will continue to be undertaken in a comprehensive and consistent manner that reflects current as well as emerging health care information policies, practices, standards, and technologies.

9.6 Alignment with Federal HIE Efforts

In parallel with the development of state-based health information exchange capabilities, the Federal government is also developing a national health information exchange identified as the NwHIN. The Federal government's intent is

that the NwHIN would connect to all 50 state-level health information exchanges in order to:

- Improve the health and healthcare of patients throughout the country, whether receiving care locally or when traveling throughout the nation
- Enhance access to additional human services. For example, the Social Security Administration and the Marshfield Clinic Research Foundation have been working together to improve the speed, accuracy, and efficiency of the federal disability application process through electronic exchange of medical evidence to adjudicate disability claims using the NwHIN Exchange
- Safeguard the privacy and security of protected health information—by fostering adoption of innovative technologies that are explored, developed, and tested in the open government environment
- Provide providers and consumers with access to vital federal health and human service partners including, but not limited to, the Centers for Medicare and Medicaid Services, the Social Security Administration, the Department of Defense Military Health System, the Veterans Administration, the Indian Health Service, and the Center for Disease Control and Prevention

WISHIN will establish necessary interfaces and alignments with the emerging NwHIN. Accordingly, WISHIN will leverage and comply with the policies, standards, and services required for statewide health information exchanges established and by the ONC. When new nationwide policies, standards, protocols, specifications, and services are adopted, WISHIN will maintain awareness of and will prioritize health information exchange policy and system updates to ensure appropriate compliance.