WISHIN

Wisconsin Statewide Health Information Network

2013

Privacy Policies

FINAL: 09/30/2013

Document Revision History

Date	Modifier	Summary of Modifications
7/23/2013	WISHIN	Original published document.
9/30/2013	WISHIN	Changes needed to ensure consistency with Participation Agreement.

Contents

Introduction

WISHIN's vision is to facilitate secure electronic sharing of the right health information at the right place and at the right time through an electronic health information exchange (HIE) to improve the health of individuals and communities in Wisconsin.

WISHIN will move Wisconsin forward toward achieving this vision and developing the health information infrastructure and interconnectivity needed for improved health care and population health. The success of the statewide HIE will be measured by its ability to enable:

- Lives to be saved and improvements in the health status of Wisconsin's population through appropriate prevention, early intervention, and treatment
- A transformation of the health care sector that creates healthy cooperation and healthy competition among providers, with patients, payers, and other partners contributing to better outcomes
- Improvement in the state's economy and competitive position as the health care sector is transformed and health care investments result in higher quality, safer, and cost-effective care

Wisconsin benefits from strong intellectual resources and a commitment to succeed in achieving statewide adoption and use of health information technology (HIT) and health information exchange (HIE) to enable improvements in the quality, safety, and efficiency of health care delivered in the state.

In order to achieve its goals, WISHIN has adopted the following privacy policies which govern the access, use, and disclosure of Protected Health Information by HIE Participants through the services being made available to Participants by WISHIN. These services are collectively referred to as the "System." WISHIN anticipates that it will review and revise these policies as needed based on the experience of WISHIN and its the Participants, and the input provided by WISHIN's advisory committees.

Definitions of Common Terms

Authorized User
An individual who has been granted access authority to the System by a Participant or by WISHIN.

Business Associate
The term Business Associate has the meaning given in Section 160.103 of Title 45, in the Code of Federal Regulations.

Patient
An individual whose Protected Health Information is part of the System, including an individual who may have chosen to opt out of his or her information being available for exchange.

Participant
Health information systems, health plans (to the degree allowed under the Participation Agreement), and other entities which provide data to the System and/or obtain and use data from the System. Participants have signed a participation agreement accepting the terms of participation and are part of the WISHIN health information exchange.

Protected Health Information (PHI)

The term Protected Health Information has the meaning given in Section 160.103 of Title 45, in the Code of Federal Regulations. The term Electronic Protected Health Information (ePHI) has the same definition, except the information is stored and/or transmitted in an electronic format.

System

The health information exchange services being made available to Participants by WISHIN.

Treatment, Payment, and/or Health Care Operations

The terms Treatment, Payment, and/or Health Care Operations have the meaning given in Section 164.501 of Title 45, in the Code of Federal Regulations.

Privacy Principles

These WISHIN Privacy Policies ("Privacy Policies") are rooted in the privacy principles discussed in the *Connecting for Health* "Architecture for Privacy in a Networked Health Information Environment."[1] Taken together with the privacy policies and procedures already deployed by Participants as covered entities under HIPAA, they form a comprehensive array of administrative safeguards addressing privacy of Protected Health Information. WISHIN has modeled its Privacy Policies on the *Connecting For Health* "Model Privacy Policies and Procedures for Health Information Exchange," with a number of differences based on state law, physical and technical safeguards available through WISHIN, and WISHIN's unique operating environment. The principles are also aligned with the core domains of the Department of Health and Human Services (DHSS) Office of the National Coordinator for Health Information Technology's (ONC) *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identified Health Information.*[2]

These core privacy principles and the policies that flow from them promote balance between individual control of and access to health information and the operational need of covered entities to take appropriate actions that do not overly restrict information uses and disclosures, such that individuals would be denied many of the benefits and improvements that information technology can bring to the health care system. The policies are intended to reflect a carefully balanced view of all of the principles and avoid emphasizing some over others in any way that would weaken the overall approach. The guiding WISHIN privacy principles are as follows:

Openness and Transparency

Openness about procedures, policies, developments, and technology concerning the handling of Protected Health Information is vital to protecting privacy. Individuals should be able to understand what information exists about them, how the personal information is used, and how they can control use of that information. Openness and transparency help promote privacy practices and gives individuals confidence with regard to privacy of Protected Health Information, which in turn can help increase consumer participation in health information networks. (ONC Domain(s): 3 - Openness and Transparency)

Purpose Specification and Minimization

Access to and use of patient health information must be limited to the type and amount necessary to accomplish specified permitted purposes. Minimizing the use of patient health

[1] http://www.markle.org/health/markle-common-framework/connecting-consumers/ct7

[2] http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_privacy_security_framework/1173

information will help decrease the amount of privacy violations, which may occur when data collected for a legitimate purpose is reused for different or unauthorized purposes.

Disclosure Limitation

Protected health information should be made available through the WISHIN System to WISHIN and Participants only by lawful means, and, if applicable, with the knowledge and permission of the individual. It is important that individuals are aware of how information concerning them is being collected in an electronic networked environment. Individuals should be educated about the potential health and treatment benefits as well as risks to their Protected Health Information that are associated with participation in the System. Individuals deciding not to participate should have the opportunity to know the System-wide effect of such decisions and the potential disadvantages. (ONC Domain(s): 5 - Collection, Use, and Disclosure Limitation)

Access and Use Limitation

Participants may use and disclose Protected Health Information obtained through the System only for purposes and uses consistent with the terms of their signed Participation Agreements. (ONC Domain(s): 5 - Collection, Use, and Disclosure Limitation)

Individual Participation and Control

Consistent with the scope of individual rights in HIPAA, individuals have the following rights regarding their Protected Health Information:

- The right to request and receive, in a timely and intelligible manner, information regarding parties who may have their specific health information, or to know the reason for a denial of such request
- The right to request to amend any Protected Health Information that they believe is inaccurate
- The right to request not to have their information available through the System

Individuals have a vital stake in personal Protected Health Information, and such rights enable them to make informed decisions about participation. These rights also provide another means to monitor for inappropriate access, use and, disclosure of Protected Health Information. Individual participation promotes information quality, privacy, and confidence in privacy practices. (ONC Domain(s): 1 - Individual Access, 2 – Correction, 4 - Individual Choice)

Data Integrity and Quality

Health information should be detailed, complete, appropriate, and current to guarantee its value to the various parties. The effective delivery of quality health care depends on complete health information. In addition, individuals can be negatively affected by inaccurate health information in other contexts, such as insurance and employment. Therefore, the System must maintain the integrity of health information and individuals must be allowed to view their health information and request to amend such health information so that it is accurate and complete. (ONC Domain(s): 6 – Data Quality and Integrity)

Security Safeguards and Controls

Security safeguards are essential to privacy protection, because they help prevent information loss, corruption, unauthorized use, modification, and disclosure. With increasing levels of cyber-crime, networked environments may be particularly susceptible without adequate security controls. Privacy and security safeguards should work together and be well

coordinated for the protection of patient health information. WISHIN's security policies are set forth in a separate System Security Policy document. (ONC Domain(s): 7 – Safeguards)

Accountability and Oversight

Privacy protections have less value to an individual if privacy violators are not held accountable for failing to follow procedures relating to such privacy protections. Potential Participants are unlikely to trust and participate in the System if they believe other Participants are not applying the same rules and being held to the same standards of accountability. System user and workforce training, privacy audits, and other oversight tools can help to identify and address privacy violations and security breaches by conditioning participation and access authority on compliance with these and the individual Participant's privacy policies, by excluding from participation those who violate privacy requirements, and by identifying and correcting weaknesses in privacy and security safeguards. (ONC Domain(s): 8 – Accountability)

Remedies

Legal and financial remedies that hold violators accountable for failing to comply with System policies must be in place for privacy protection. Such remedies will give individuals confidence in the WISHIN's commitment to keeping Protected Health Information private, and mitigate any harm that privacy violations may cause individuals. As a condition of continued participation, all Participants in the System must have a common duty to participate in investigation, mitigation, and remediation steps for the integrity of the System. (ONC Domain(s): 8 – Accountability)

Reliance on Participant Policies and Enforcement

While WISHIN should have a number of core policies and procedures for the benefit and confidence of all Participants, WISHIN should not try to replace policies, procedures and methods already adopted by Participants as covered entities under HIPAA and in accordance with other applicable laws. WISHIN should identify, disseminate, and enforce only those policies and procedures necessary for protecting the quality and integrity of the System and coordinate responses to privacy incidents. WISHIN recognizes that existing Participant policies govern in all other areas.

These ten principles underlie the WISHIN privacy policies. Given the advanced level of technology available to most organizations, a majority of the policies should be relatively manageable to implement. In some cases, however, organizational and technical barriers may restrict an organization's ability to implement the policies. For example, the System does not currently allow a patient to access the System and see an audit trail of those parties that have requested information about the patient. Patients could potentially benefit from such information, and such options should be implemented to promote the principles of openness and transparency, security safeguards and controls, purpose specification and minimization, disclosure limitation, collection limitation, and accountability.

The creation of a networked electronic health information environment will provide for more efficient and effective delivery of patient care. However, the creation of an electronic network that includes a massive volume of Protected Health Information that can be easily collected and disseminated must have adequate privacy and security measures. WISHIN policies incorporate principles outlined in the ten principles as well as basic requirements set forth in HIPAA and other applicable laws. The WISHIN policies seek to achieve a balance between maintaining the confidentiality of health information and maximizing the benefits of such information.

Status of WISHIN and Participants

All Participants are covered entities under HIPAA or agree to be contractually bound to follow all HIPAA rules and regulations as though they were a covered entity. WISHIN is a Business Associate of the Participants. WISHIN accepts and agrees to follow terms applicable to the privacy of Protected Health Information by virtue of its business associate agreement with each Participant and these privacy policies.

Effect of Legislation and Rule Changes

WISHIN and Participants need to remain flexible in order to adapt to the uncertainty of state and federal legislation and regulations that will affect design, safeguards, rights, and responsibilities over time. This shall include monitoring and implementing design components and safeguards mandated in the Health Information Technology for Economic and Clinical Health Act or "HITECH" as enacted in Public Law 111-5, and any regulations issued thereunder.

WISHIN policies and the health information technology design components and safeguards need to be developed in accordance with Wisconsin Statutes, for example, Wisconsin Statutes §51.30, limiting release of alcohol, drug abuse, developmental disabilities, and mental health treatment records, and Wisconsin Statutes Sec §252.15, restricting release of HIV test results in cases of "significant exposure," as well as federal regulations, such as 42 CFR Part 2, addressing the confidentiality of patient records from federally-assisted alcohol and drug abuse programs.

Safeguards in a Health Information Exchange Environment

HIPAA permits covered entities that hold Protected Health Information to disclose such information to other covered entities both for their own purposes of Treatment, Payment, and Health Care Operations and for the purposes of Treatment, Payment, and Health Care Operations of those other covered entities*, without written authorization.*[3] HIPAA limits authority to disclose without authorization in other situations. HIPAA thus places a duty on Participants holding Protected Health Information to determine that each proposed disclosure is permitted.

In a non-electronic networked environment, Participants subject to this duty would have the opportunity to examine third party requests for information beforehand and make an individual determination whether a disclosure is a permitted disclosure for the Treatment, Payment, or Health Care Operations purposes of the requesting Participant. In an electronic networked environment, such as WISHIN, the disclosing Participant will not receive or "process" a request for access. Other Participants using the record locator service can simply locate the Participant's record and access it as needed. The human element of analyzing individual requests is absent.

Accordingly, to permit Participants that furnish information to meet their obligation to disclose Protected Health Information only for a qualifying purpose, and to meet certain other conditions, all Participants commit to accessing PHI only as permitted by the terms of the Participation Agreement.

WISHIN and all Participants are also subject to the additional regulations and penalties in Wisconsin Statutes §51.30, which deals with restrictions on release of patient records related to alcohol, drug abuse, developmental disabilities, and mental health treatment, and Wis. Stats. §252.15, restricting release of HIV test results, as well as federal regulations, such as 42 CFR Part 2, restricting disclosure and use of alcohol and drug abuse patient records.

[3] 45 C.F.R. §§164.506(c)(3) and (4).

Policy 100: Compliance with Law and Policy

ONC Domain: Collection, Use and Disclosure Limitation

Scope and Applicability: This Policy applies to WISHIN and all Participants.

Policy:

Laws

Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of Protected Health Information and establishing certain individual privacy rights. Each Participant shall use reasonable efforts to stay abreast of any changes or updates to, and interpretations of, such laws and regulations, and take appropriate steps to be in compliance of such laws.[4]

Each Participant that is a HIPAA "covered entity" or "business associate" is thus subject to both its individual legal duty as a regulated covered entity or business associate under HIPAA and its contractually assumed obligations under its Participation Agreement. All other Participants are similarly obligated to comply with the provisions of the Participation Agreement and all applicable privacy laws, including complying with HIPAA privacy and security requirements relating to the protection, disclosure, and use of PHI, as if the Participant was a "covered entity."

Participant Policies

Each Participant is responsible for ensuring that it has the appropriate and necessary internal policies for compliance with applicable laws.

User Criteria

Each authorized user derives his or her permission to access and use the System from a Participant. Therefore each authorized user must maintain a current relationship to a Participant in order to use the System. Authorized users must therefore be: (i) Participants (for example, an individual physician) or workforce of a Participant, (ii) an individual Business Associate or workforce of such Business Associate, (iii) a properly authorized individual contractor or subcontractor of a Business Associate or workforce of such contractor or subcontractor, or (iv) a physician on the medical staff of a Participant who does not meet the criteria referenced in (i), (ii) or (ii), above. Additionally, Participants that are covered health plans, although not authorized users, may have access to reports generated from the system. Such covered health plans shall comply with these policies and procedures.

Application to WISHIN Employees

WISHIN shall ensure that its employees and subcontractors shall, at all times, comply with these WISHIN policies and all applicable federal, state, and local laws and regulations including, but not limited to, those protecting the confidentiality and security of Protected Health Information and

[4] The Participants acknowledge the need to revise Policies and certain other technical and administrative features to conform to HITECH and regulations to be promulgated thereunder. These changes will be made in due course.

establishing certain individual privacy rights. WISHIN will appoint a Privacy Officer, consistent with the provisions of its System Security Policies.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their Business Associates and to the contractors and subcontractors of their Business Associates as they deem appropriate and as required by law through the terms of their business associate agreements.

Policy 200: Notice of Privacy Practices

ONC Domain: Openness and Transparency

Scope and Applicability: This Policy applies to all Participants.

Policy:

To maintain openness and transparency, Participants who are health care providers are encouraged to include information about their participation in the health information exchange and what that means to patients in their communications about privacy practices to their patients.

Content

The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule[5] and comply with applicable laws and regulations. Participants shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of Protected Health Information through the System. WISHIN provides the following sample language for Participants who elect to amend their Notice:

> *"In compliance with federal and state laws, we may make your Protected Health Information available electronically through an electronic health information exchange to other health care providers and health plans that request your information for purposes of Treatment, Payment, and Health Care Operations; and to public health entities as permitted by law. Participation in an electronic health information exchange also lets us see other providers' and health plans' information about you for purposes of Treatment, Payment, and Health Care Operations."*

Dissemination and Individual Awareness

Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgment of receipt by the individual,[6] which policies and procedures shall comply with applicable laws and regulations.

Participant Choice

Participants may choose a more proactive Notice distribution or patient awareness process than provided herein and may include more detail in their Notice, so long as any expanded detail does not misstate the safeguards supporting the System.

[5] 45 C.F.R. §§ 164.520(b).

[6] See 45 C.F.R. §§164.520(c)(2)(ii).

Policy 300: Individual Control of Information Available Through the System

ONC Domain: Individual Choice

Scope and Applicability: This Policy applies to WISHIN and all Participants.

Policy:

Information Available in the System

Participants will provide health information data to an edge server, which is either centrally located or located in the Participant's own facility. WISHIN will maintain a centralized basic master patient index of demographic information with pointers to individuals' health information on the edge server(s). Participants will then query the master patient index to locate health information from other Participants as needed. All patients will begin opted in to WISHIN Pulse, but information marked confidential will not be viewable. WISHIN will maintain an individual's election to opt out, described below, as part of the master patient information.

Individual's Choice to Opt Out of System versus Request for Restriction under HIPAA

WISHIN gives individuals the choice to opt out of having their health information viewable by Participants in the System. This is separate from the patient's right under HIPAA to ask a health care provider to restrict the sharing of the patient's health information. Participants remain responsible for handling requests for restrictions under HIPAA.

Processing Opt Out Requests

Individuals will make a choice to opt out by submitting a completed Patient Choice form to WISHIN by regular mail. The patient choice form will be processed by WISHIN. Once the individual's opt out request has been processed, that individual's health information will not be available to other Participants in the System, except in the limited circumstances described below.

Participants will not be responsible for administering an individual's requests to opt out of the System. Participants will not be responsible for receiving or processing an individuals' Patient Choice forms, or for blocking, filtering out or flagging health information for individuals who ask to opt out of the System. Participants will send all of the required health information though the System (including the information of individuals who opt out).

Informing Patients of the Choice to Opt Out.

Participants agree to inform individuals (through whatever means they deem appropriate) about their right to opt out of the System. WISHIN will provide information to Participants for this purpose as follows:

1. WISHIN will, from time to time, furnish Participants that are health care providers with an informational brochure about the System, which can be distributed to individuals to explain the meaning and effect of participation or opting out. The brochure will also contain a link to the WISHIN website where WISHIN will provide an explanation of the meaning and effect of participation or opting out and a tool for opting out or revoking a prior opt out election. WISHIN will make the brochure available on its website at: wishin.org.

2. The brochure shall explain the System-wide scope of an opt out decision, the risks to the individual's data privacy and security if the individual participates, the effect and benefits of participation, and the effect and disadvantages of opting out. The brochure will explain that certain information is prohibited by federal and state law from being part of the exchange. The brochure will explain that a Participant's policies continue to govern access, use, and disclosure in all other contexts.
3. The brochure shall explain that, even if an individual chooses to opt out of having his or her health information available in the System, certain health information will still continue to be sent to particular government entities (such as public health), as permitted by law. An individual's health information may also be accessed in an emergency situation where health information is necessary for treatment and the individual is unable to give consent.
4. The brochure shall state that the Participant (and other Participants) will not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her exchanged through the System.
5. Participants may furnish the brochure to individuals at the initiation of an episode of care and inform individuals of the opportunity to opt out or ask questions. Each Participant may have one or more persons designated to answer questions about the System or about opting out or revoking a prior opt out election.
6. Participants may also direct individuals to the WISHIN website and to a help line at WISHIN where the individual can ask additional questions and obtain additional information about participation in WISHIN and opt out. WISHIN as a business associate of the Participants is authorized to provide information and answer individual questions about WISHIN and the opt out alternative on behalf of Participants.
7. An individual's election to opt out of participation in the System must be communicated by the individual to WISHIN in the manner provided by WISHIN. Once WISHIN has processed the opt out request, the opt out will be in effect System-wide with regard to that individual's information.

Change to Prior Election

An individual may opt out or revoke a prior election to opt out at a later date. The brochure and information on the WISHIN website should inform the individual that revoking a prior opt out election will result in information that was previously unavailable through the System becoming available to all Participants using the System.

Effect of Choice

An individual who opts out of the System opts out as to all of his or her records made available through the System, not just with respect to a particular Participant or episode of care. The effect is System-wide. An individual's election to opt out, whether made at the time of service or subsequently, will have prospective effect only and will not impact access, use, and disclosure occurring before the decision is received and processed through the System.

Individual's Choice to Opt Out a Minor

A legal guardian or parent may choose to have his or her minor child's records opted out of the System. When the minor child reaches the age of Majority, WISHIN will send a notice to said minor child at his/her last known address, informing the child of his or her current opt out status, and

providing the child with the option of opting his or her records back into the System. WISHIN will not automatically opt in a minor who has previously been opted out by a parent or guardian.

Limited Effect of Opt Out

A decision to opt out only affects the availability of the individual's Protected Health Information through the System. Each Participant's policies continue to govern access, use and disclosure in all other contexts and via all other media.

Individual's Choice

Participants shall establish reasonable and appropriate processes to enable the exercise of the individual's choice not to have information about him or her included in the System. The uniform processes described in this Policy are not exclusive, and Participants may adopt additional, but not inconsistent, mechanisms.

Reliance

Participants will be entitled to assume that an individual has not opted-out if the individual's Protected Health Information is available through the System.

Incompetence or Incapacity

Unless WISHIN has been specifically notified of an individual's incompetence or incapacity, WISHIN may presume that an individual is competent to exercise his or her rights under this Policy (unless such individual is a minor).

Individual's Access to Information in the System

As stated in Policy 1200, WISHIN does not maintain ownership of the data contributed to the System. All data is owned by the Participants contributing the information. Therefore, if an individual requests copies of his/her PHI in the System, WISHIN will direct the individual to contact the Participant(s) who have contributed data to the System. Upon an individual's request, WISHIN may provide the individual with a list of the Participants who have contributed PHI about him or her, to aid the individual in obtaining the information from Participants.

Policy 400: Access to, Use, and Disclosure of Information

ONC Domain: Collection, Use and Disclosure Limitation

Scope and Applicability: This Policy applies to WISHIN and all Participants.

Policy:

Compliance with Law

Participants shall access, use, disclose, and/or dispose of Protected Health Information through WISHIN only in a manner consistent with all applicable federal, state, and local laws and regulations and not for any unlawful or discriminatory purpose.

Documentation and Reliance

If applicable law requires that certain documentation exist or that other conditions be met prior to disclosing or accessing Protected Health Information for a particular purpose, the disclosing or accessing Participant shall obtain the required documentation or met the requisite conditions. Each access, use, or disclosure of Protected Health Information by a Participant is a representation to every other Participant in the System that the health information being accessed, used, or disclosed has met all prerequisites under state and federal law for such access, use, or disclosure.[7]

Purposes

A Participant may request and use Protected Health Information through the System only for the purposes set forth in the Participation Agreement, and only to the extent necessary and permitted by applicable federal, state, and local laws and regulations, these Policies, and the Participation Agreement.[8] A Participant may request and use Protected Health Information through the System only if the Participant has or has had or is about to have the requisite relationship to the individual whose Protected Health Information is being accessed and used.

Participant Policies

Participant uses and disclosures of, and requests for, Protected Health Information through the System shall comply with WISHIN Policies 500 and 600, dealing with information subject to special protection and the minimum necessary requirements.[9]

Each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.

Subsequent Use and Disclosure

A Participant that has accessed information through the System and merged the information into its own record shall treat the merged information as part of its own records and thereafter use and

[7] 45 C.F.R. § 164.530(j).

[8] 45 C.F.R. § 164.502(a), (b).

[9] 45 C.F.R. § 164.502(b).

disclose the merged information only in a manner consistent with its own information privacy policies and laws and regulations applicable to its own records. A Participant shall not access Protected Health Information through the System for the purpose of disclosing that information to third parties, other than for the Permitted Purposes outlined in the Participation Agreement.

Disclosures to Law Enforcement

If a law enforcement official requests PHI from WISHIN via a court order, warrant, patient authorization, or other valid legal process, WISHIN will attempt to direct the requesting entity to the Participant(s) who owns the information subject to the request, if applicable. However, in the event the request is still directed at WISHIN or the request is for information that may only be available through the exchange, WISHIN may then provide the requested PHI as required by and in accordance with city, state, and federal law without first obtaining specific patient authorization. Some examples of circumstances in which WISHIN may provide information to law enforcement include:

1. Demographic information to assist in the identification or location of a suspect, fugitive, material witness, or missing person;
2. Regarding a patient who is or is suspected to be a victim of a crime;
3. If WISHIN believes the PHI requested constitutes evidence of criminal conduct that occurred on the premises of WISHIN;
4. In emergency situations, to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime;
5. It is aggregate data that could not be easily obtained by a law enforcement request to individual Participant(s);
6. It is information stored only by WISHIN, such as audit logs or reports of access to information;

-and-

A. If the PHI sought is relevant and material to the law enforcement inquiry;
B. The request is specific and limited in scope to the extent reasonably practicable;
C. De-identified PHI could not be used; and
D. The court order, warrant, patient authorization, or other legal process complies with Wisconsin law which in some cases requires patient authorization to release.

If a WISHIN employee is presented with a court order, warrant, patient authorization, or other legal process, the employee will immediately notify the Privacy Officer and/or WISHIN legal counsel of the request. The Privacy Officer and/or WISHIN legal counsel will evaluate the request and determine whether and how the disclosure will be made. No PHI will be disclosed in response to a court order, warrant, patient authorization, or other legal process prior to discussing the document with the Privacy Officer and/or legal counsel.

The person providing PHI in response to a court order, warrant, patient authorization, or other legal process is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided, the agency name and address (if known), the date the PHI was provided, and a brief summary of the PHI provided for each patient whose PHI is reported or released.

Documentation of releases and disclosures that are made in response to a court order, subpoena, warrant, summons, or other similar document may be maintained by the WISHIN Privacy Officer. All documentation relating to requests for a patient's PHI shall be maintained for a minimum of six (6) years.

Responding to Inquiries from National Security, Intelligence, and Protective Services Officials

If a federal official requests PHI from WISHIN for intelligence, counter-intelligence, or other national security activities, WISHIN may provide the requested PHI as required by and in accordance with city, state, and federal law without first obtaining specific patient authorization. The WISHIN employee receiving such request will immediately contact the WISHIN Privacy Officer.

The person providing PHI to authorized federal officials for national security and intelligence activities and protective services is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided, the agency name and address, the date the PHI was provided, and a brief summary of the PHI provided for each patient whose PHI is reported or released.

Documentation of releases and disclosures that are made to authorized federal officials for national security and intelligence activities and protective services shall be maintained by the Privacy Officer. All documentation relating to requests for a patient's PHI will be maintained for a minimum of six (6) years.

Accounting of Disclosures

Each Participant shall be responsible to account only for its own disclosures. WISHIN shall provide a means by which each Participant requesting information will indicate the purpose and use for such request so that Participants that disclose information may document the purposes for which they have made disclosures for use in an accounting or as otherwise requested by the Participant.[10] Unless a Participant requesting information notes otherwise, each request by a Participant that is a provider is deemed to be for such Participant's treatment purposes. Each Participant requesting information shall provide information required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement.

[10] 45 C.F.R. § 164.502(b).

Audit Logs

WISHIN shall provide an audit log to document which Participants posted and accessed the information about an individual through the System and when such information was posted and accessed.[11] Upon request of a Participant, WISHIN shall provide such periodic and/or one-time reports as are necessary to determine and/or document user access including what information was accessed by a given user and when such information was accessed.

Authentication

WISHIN shall follow a uniform authentication requirement for verifying and authenticating the identity and authority of each authorized user and Participant.[12,13] Participants shall be entitled to rely on WISHIN's user access and authorization safeguards and may assume an authorized user making a request for Protected Health Information on behalf of a Participant is authorized to do so. This process is described in greater detail in the WISHIN Security Policies.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their Business Associates and to the contractors and subcontractors of their Business Associates as they deem appropriate and as required by law through the terms of their business associate agreements.

[11] See 45 C.F.R. §§ 164.316, 164.308(a)(1)(i).

[12] See 45 C.F.R. §§ 164.514(h), 164.312(d).

[13] See **Connecting for Health**, "Authentication of System Users."

Policy 500: Information Subject to Special Protection

ONC Domain: Collection, Use and Disclosure Limitation

Scope and Applicability: This Policy applies to WISHIN and all Participants.

Policy:

Special Protection for Sensitive Data

Both federal and state laws extend special protection to certain types of health information that WISHIN refers to as "sensitive data" or "sensitive health information." "Sensitive data" is health information that falls outside the general rule that health care providers can access and use patient health information for treatment purposes without patient authorization. In some cases, these state and federal laws impose different or more stringent requirements regarding the sharing of patient information than the requirements imposed by HIPAA. Other health information may be subject to special safeguards under a Participant's policies, even if not legally required.

WISHIN facilitates compliance with the state and federal laws that provide special protection to sensitive data as follows:

Sensitive Data Will Be Disclosed Only in a Medical Emergency.

"Sensitive data" or "sensitive health information" means, for example, health data that is subject to Section 51.30 of the Wisconsin Statutes (i.e., mental health, AODA or developmental disabilities information) or other health data that the disclosing Participant has identified as "sensitive" under its own policies. Sensitive Data will be released through the System to a Participant only when the Participant has certified that the subject individual has a medical emergency and cannot provide consent.

Prominent Identification of Sensitive Data and Prohibition on Re-Disclosure; Reporting of Release of Sensitive Data. If a Participant releases any Sensitive Data into the System, the Participant must prominently identify the health data as being Sensitive Data, in accordance with WISHIN's related Policies and Procedures, before the data is sent to WISHIN Pulse. Information flagged as "sensitive" will only be available through WISHIN Pulse in an emergency when the patient cannot provide consent.

Notation of Disclosure in Patient's Records. WISHIN shall maintain a separate Sensitive Data disclosures audit log for each Participant that will include the name of the person to whom the Sensitive Data was released, their affiliation to any health care facility, and the date of the release. A Participant who discloses the Sensitive Data must access the Sensitive Data disclosures audit log in order to update the patient's records to reflect the disclosure.

Some Information Must Not be Shared through WISHIN Pulse

Some information subject to special protection under state and federal laws must not be shared through WISHIN Pulse. Participants are responsible for identifying this information and assuring that it is not sent through WISHIN Pulse. Examples of information that Participants must not share through WISHIN Pulse:

No Psychotherapy Notes, AODA Records Maintained in Connection with a Federally Assisted AODA Program, or Records of HIV Results From a Compelled Test. Participants shall not release into the System any (1) "psychotherapy notes," as defined in HIPAA, 45 CFR §164.501, or (2) HIV test results from a test that

was compelled under Section 252.15(5g) of the Wisconsin Statutes as a result of "significant exposure." Participants also shall not release into the System any records subject to 42 CFR Part 2 (i.e., AODA treatment records maintained in connection with a federally-assisted AODA program), unless the WISHIN Policies and Procedures are amended to expressly permit the release of such records.

Each Participant is responsible for complying with applicable laws and its own policies with regard to identifying and providing special treatment for information subject to special protection. Participants will refer to federal, state and local laws for full restrictions on sharing and accessing information subject to special protection.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their Business Associates and to the contractors and subcontractors of their Business Associates as they deem appropriate and as required by law through the terms of their business associate agreements.

Policy 600: Minimum Necessary

ONC Domain: Collection, Use, and Disclosure Limitation

Scope and Applicability: This Policy applies to WISHIN, all Participants and their Business Associates and contractors.

Policy:

Requests

Each Participant shall request only the minimum amount of health information through the System as is necessary for the intended purpose of the request. This requirement does not apply to Participants requesting health information for purposes of treatment.

Disclosures

A Participant is entitled to rely on the scope of a requesting Participant's request for information as being consistent with the requesting Participant's minimum necessary policy and needs.

Workforce, Business Associates, and Contractors

Each Participant shall adopt and apply policies to limit access to the System to members of its workforce who qualify as authorized users and only to the extent needed by such authorized users to perform their job functions or duties for the Participant.

Entire Medical Record

A Participant shall not use, disclose, or request an individual's entire medical record unless necessary and justified to accomplish the specific purpose of the use, disclosure, or request.

Application to Health Plans

Health Plans are only provided information from WISHIN Pulse as defined in the approved use cases in the Participation Agreement.

Application to Providers and Treatment Purposes

While this minimum necessary policy is not required by HIPAA for providers accessing, using, and disclosing health information for treatment purposes, they are encouraged to follow it when consistent with treatment needs.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their Business Associates and to the contractors and subcontractors of their Business Associates as they deem appropriate and as required by law through the terms of their business associate agreements.

Policy 700: Workforce, Business Associates, and Contractors

ONC Domain: Collection, Use, and Disclosure Limitation
Safeguards
Accountability

Scope and Applicability: This Policy applies to WISHIN and all Participants and their business associates and contractors.

Policy:

WISHIN Responsibility

WISHIN is responsible to establish and enforce policies designed to comply with its responsibilities as a Business Associate under HIPAA and to train and supervise its workforce to the extent applicable to their job responsibilities.

Participant Responsibility

Each Participant is responsible to establish and enforce policies designed to comply with its responsibilities as a covered entity under HIPAA and a Participant in the System, and to train and supervise its authorized users to the extent applicable to their job responsibilities.

Authorized Users/End User License Agreement

All authorized users, whether members of a Participant's workforce, member of the workforce of a Business Associate or contractor, shall execute an individual end user license agreement which is displayed to them during their initial log-in to the System. Through the end user license agreement, the authorized users will acknowledge familiarity with and acceptance of the terms and conditions on which their access authority is granted. This shall include familiarity with applicable privacy and security policies of the Participant, Business Associate, or contractor, as applicable. Participants shall determine to what extent members of their workforce or the workforce of Business Associates and contractors require additional training on account of the Participant's obligations under their participation agreement, and arrange for and document such training. WISHIN shall reserve authority in the Participation Agreement to suspend, limit, or revoke access authority for any authorized user or Participant for violation of Participant and/or WISHIN privacy and security policies.

Access to System

Each Participant shall allow access to the System only by those authorized users who have a legitimate and appropriate need to use the System and/or release or obtain information through the System. No workforce member, agent, or contractor shall have access to the System except as an authorized user on behalf of a Participant and subject to the Participant's privacy and security policies and procedures and the terms of the individual's user agreement.

Corrective Actions for Non-Compliance

Each Participant shall implement procedures to hold authorized users, business associates and contractors accountable for following the Participant's policies and procedures and for requiring that they do not use, disclose, or request health information except as permitted by the participation agreement.[14] Such corrective action measures may include, but not be limited to, retraining, verbal and written warnings, demotion, and/or termination.

Reporting of Non-Compliance

Each Participant shall have a procedure, and shall require all workforce members, Business Associates and contractors to report any non-compliance with the Participant's policies or the policies applicable to authorized users.[15] Each Participant also shall establish a mechanism for individuals whose health information is included in the System to report any non-compliance with these Policies or concerns about improper disclosures of Protected Health Information.

Enforcing Business Associate Agreements and Contractor Agreements

Each Participant shall require in any relationship with a Business Associate, contractor, or other third party (which may include staff physicians) that will result in such third party becoming an authorized user on behalf of the Participant, or that will result in members of the workforce of such third party becoming an authorized user on behalf of the Participant, that: (i) such third party and any member of its workforce shall be subject to these Policies and to the terms of the Participation Agreement when accessing, using or disclosing information through the System, and (ii) that such third parties and/or authorized users on its workforce may have their access suspended or terminated for violation of these Policies or other terms and conditions of the authorized user agreement. Nothwithstanding the forgoing, in no event shall Participant be responsible for the acts or omissions of any non-employed physician.

[14] 45 C.F.R. § 164.530(e).

[15] 45 C.F.R. § 164.530(a), (d).

Policy 800: Amendment of Data

Domain: Correction
Data Quality and Integrity

Scope and Applicability: This Policy applies to WISHIN and all Participants.

Policy:

Accepting Amendments

Each Participant shall comply with applicable federal, state, and local laws and regulations regarding individual rights to request amendment of health information.[16] If an individual requests, and the Participant accepts, an amendment to the health information about the individual, the Participant, assisted by WISHIN, shall make reasonable efforts to inform other Participants that accessed or received such information through WISHIN, within a reasonable time. Only the Participant responsible for the record being amended may accept an amendment. If one Participant believes there is an error in the record of another Participant, it shall contact the responsible Participant.

Informing Other Participants

A Participant shall notify WISHIN using a method established by WISHIN for such purpose when it has amended an individual's Protected Health Information. WISHIN shall cooperate in identifying other Participants who have accessed the information in its pre-amendment form. WISHIN shall then be responsible to notify such other Participants of the amendment.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their Business Associates and to the contractors and subcontractors of their Business Associates as they deem appropriate and as required by law through the terms of their business associate agreements.

[16] 45 C.F.R. § 164.526.

Policy 900: Requests For Restrictions

ONC Domain: Individual Choice

Scope and Applicability: This Policy applies to all Participants.

Policy:

Data Provider Responsibility

If a Participant agrees to an individual's request for restrictions,[17] as permitted under the HIPAA Privacy Rule, such Participant shall comply with the restrictions. This shall include not making the individual's information available to the System if required by the restriction. When evaluating a request for a restriction, the Participant shall consider the implications that agreeing to the restriction would have on the accuracy, integrity and availability of information through the System.

Recipient Responsibility

A Participant when accessing data as a data recipient shall not be expected to know of or comply with a restriction on use or disclosure agreed to by a Participant that provides data.

[17] Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 45 C.F.R. § 164.522. For example, an individual could request that information not be used or disclosed for a particular purpose or that certain information not be disclosed to a particular individual. Covered entities are not required to agree to such requests under HIPAA.

Policy 1000: Privacy Breaches – Investigations and Mitigation

ONC Domain: Safeguards
Accountability

Scope and Applicability: This Policy applies to WISHIN, all Participants and their Business Associates and contractors.

Policy:

Individual Complaints

Any individual may submit a complaint about an access, use, or disclosure of PHI through the System to WISHIN, the Participant that maintains the PHI, or the Secretary of the Department of Health and Human Services (HHS) in Washington, DC. If the individual wants to file a formal complaint with WISHIN, he or she should be directed to the WISHIN Privacy Officer. If the individual wants to file his/her complaint with the Secretary of HHS, he/she should be directed to the Office for Civil Rights website (www.hhs.gov/ocr/hipaa). The WISHIN Privacy Officer will document each privacy complaint received including in the documentation a brief description of and/or the basis for the complaint.

The Privacy Officer will supplement the initial documentation to include documentation of the investigation and any actions taken in response to the complaint. All documentation relating to the individual's complaint will be maintained for a minimum of six (6) years.

Duty to Investigate

Each Participant shall promptly investigate reported or suspected privacy breaches of Participant's System interface. Upon learning of a reported or suspected breach, the Participant shall notify WISHIN and any other Participant whom the notifying Participant has reason to believe is affected or may have been the subject of unauthorized access, use, or disclosure. WISHIN shall have the right to participate in the investigation and to know the results and any remedial action taken, except that WISHIN need not be notified of specific workforce disciplinary actions short of termination of an employee.

Each investigation shall be documented. At the conclusion of an investigation, a Participant shall document its findings and any action taken in response to an investigation. A summary of the findings shall be sent to WISHIN. WISHIN may use examples of breaches for education and for policy and other safeguard development; however, WISHIN will not disclose the names of individuals or organizations involved in the breach.

Incident Response

WISHIN shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by Participants or discovered by WISHIN. The incident response system shall include the following features, each applicable as determined by the circumstances:

1. Cooperation in any investigation conducted by the Participant or direct investigation by WISHIN;
2. Notification of additional Participants or authorized users as needed to prevent further harm or to enlist cooperation in the investigation and/or mitigation of the breach;
3. Cooperation in any mitigation steps initiated by the Participant;

4. Furnishing audit logs and other information helpful in the investigation;
5. Developing and disseminating remediation plans to strengthen safeguards or hold Participants or authorized users accountable;
6. Where appropriate, take steps to comply with the HIPAA Breach Notification Rule;[18]
7. Any other steps mutually agreed to as appropriate under the circumstances; and
8. Any other steps required under the incident reporting and investigation system contained in the WISHIN Security Policies.

Cooperation in Investigations

WISHIN shall cooperate with a Participant in any investigation of the Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by the Participant, when the investigation implicates WISHIN conduct, or the conduct of another Participant or authorized user, or the adequacy or integrity of System safeguards.

Each Participant shall cooperate with WISHIN in any investigation of WISHIN or of another Participant into WISHIN's or such other Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by WISHIN or the other Participant, when the investigation implicates such Participant's compliance with WISHIN policies or the adequacy or integrity of System safeguards.

Non-retaliation for Filing a Complaint

WISHIN will not intimidate, threaten, coerce, discriminate, penalize, or take other retaliatory action against an individual who exercises his/her rights under HIPAA or against any individual who participates in a process governed by the Privacy Regulations. This prohibition also applies to:

1. Individual complaints filed with WISHIN, a Participant, or the Secretary of HHS;
2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing arising under the HIPAA Privacy Regulations; or
3. Opposing any act or practice of WISHIN, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not disclose PHI in violation of the HIPAA Privacy Regulations, or otherwise violate applicable law.

No Waiver

No individual will be asked to waive his/her HIPAA rights, including the right to file a complaint about the use or disclosure of his/her PHI.

Duty to Mitigate

Each Participant shall implement a process to mitigate, and shall mitigate to the extent practicable, the harmful effects that are known to the Participant of a violation of applicable laws, regulations, and/or these policies related to the unauthorized access, use, or disclosure of Protected Health Information through the System, and that is caused or contributed to by the Participant or its workforce members, agents, and contractors. Steps to mitigate could include, but are not limited to,

[18] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, §13402, and its implementing regulations

Participant notification to the individual or Participant request to the party who improperly received such information to return and/or destroy impermissibly disclosed information.

Cooperation in Mitigation

A Participant that has caused or contributed to a privacy breach or that could assist with mitigation of the effects of such breach shall cooperate with WISHIN and with another Participant that has the primary obligation to mitigate a breach in order to help mitigate the harmful effects of the breach. This obligation exists whether the Participant is directly responsible or whether the breach was caused or contributed to by members of the Participant's workforce or by its Business Associates or contractor or their workforce.

Notification to WISHIN

A Participant primarily responsible to mitigate shall notify WISHIN of all events related to the System requiring mitigation and of all actions taken to mitigate. In the event the mitigation results in termination of an employee, the Participant has the responsibility to notify WISHIN of the name of the individual whose employment was terminated.

WISHIN may facilitate the mitigation process if asked. WISHIN may use examples of breaches for education and for policy and other safeguard development; however, WISHIN will not disclose the names of individuals or organizations involved in the breach.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their Business Associates and to the contractors and subcontractors of their Business Associates as they deem appropriate and as required by law through the terms of their business associate agreements.

If the WISHIN Privacy Officer determines that PHI that was wrongfully accessed, used, or disclosed is created or maintained by a subcontractor of WISHIN, the HIPAA Privacy Officer will notify the subcontractor of the results of the investigation and any required action on the part of the subcontractor. If the results of the investigation are that the WISHIN subcontractor inappropriately accessed, used, or disclosed an individual's PHI, the WISHIN Privacy Officer will prepare a recommendation for the WISHIN Board as to whether the relationship between the subcontractor and WISHIN should continue.

Mitigation by WISHIN

If an investigation of a privacy breach indicates that PHI was misused or improperly disclosed, the WISHIN Privacy Officer shall determine:

1. What, if any, privacy practices at WISHIN require modification;
2. Whether a new policy, procedure, or form should be developed or whether an existing policy, procedure, or form should be revised;
3. Whether additional training is required to avoid a repeat violation;
4. What corrective actions, if any, will be imposed against the individual who committed the violation.

Policy 1100: Authorized User Controls

ONC Domain: Safeguards
Accountability

Scope and Applicability: This Policy applies to WISHIN, all Participants and their Business Associates and contractors. This Policy is to be read and applied in conjunction with the WISHIN Security Policies.

Policy:

Participant Responsibilities

Each Participant is responsible to:

1. Designate its responsible contact person who shall be initially responsible on behalf of the Participant for compliance with these policies and to receive notice on behalf of the Participant. For Participants that have their own system administrator, this shall ordinarily be the system administrator.
2. Designate its own authorized users from among its workforce, and designate Business Associates and contractors authorized to act as (or designate from among their workforce) authorized users on its behalf.
3. Train and supervise its authorized users and require any Business Associate or contractor to train and supervise its authorized users consistent with the Participant's privacy policies, the Business Associate Agreement, and all applicable state and federal laws, as applicable.
4. In the case of Participants with a System Administrator, immediately suspend, limit or revoke access authority upon a change in job responsibilities or employment status of an authorized user. Revocation shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant.
5. For Participants without their own System Administrator, immediately notify WISHIN of the change so that WISHIN may revoke access authority. Notification shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant.
6. Take such disciplinary action as it may deem appropriate against any Authorized User who violates the confidentiality provisions of this Agreement or the Policies and Procedures;

WISHIN Responsibilities

WISHIN is responsible to:

1. Grant access authority to individuals designated by a Participant, subject to reserved authority to suspend, limit, or revoke such access authority as described later.
2. Train and supervise its own authorized users on these policies and the standard terms required by its Business Associate Agreement with Participants.
3. Provide appropriate audit reports to Participants to allow them to review and investigate their authorized users' activities in the exchange to review compliance with these policies.

4. Suspend, limit or revoke access authority for its own authorized users or any authorized user who is a member of the workforce of any subcontractor of WISHIN as required by these policies or the terms of its Business Associate Agreement in the event of breach or non-compliance.
5. Immediately revoke access authority upon a change in job responsibilities or employment status of its own authorized users or the authorized user of its subcontractor.
6. Suspend, limit, or revoke the access authority of an authorized user on its own initiative upon a determination that the authorized user has not complied with the Participant's privacy policies, WISHIN policies or the terms of the user agreement, if WISHIN determines that doing so is necessary for the privacy of individuals or the security of the System.

WISHIN Security Policy

The details of how to grant and revoke access authority are contained in the WISHIN Security policy.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their Business Associates and to the contractors and subcontractors of their Business Associates as they deem appropriate and as required by law through the terms of their business associate agreements.

Policy 1200: Ownership and Modification of Data in the System

ONC Domain: Data Quality and Integrity

Scope and Applicability: This Policy applies to WISHIN, all Participants and their Business Associates and contractors.

Policy:

Ownership of Data

Each Participant shall remain the owner of the data it makes available to the System, and each Participant shall be responsible for the quality and integrity of the data it contributes to the system.

WISHIN shall not modify any data in the System owned by Participants. However, WISHIN may:

- Modify the rendering of that data for consistency of display in the System, based on Participant-approved specifications.
- Create de-identified or specially-configured feeds of that data for reporting and other purposes set forth in the Participation Agreement

None of the above permitted uses will modify the data the Participants contribute to the system, just the rendering of it or new reporting feeds based on the data originally submitted.

Master Patient Index

WISHIN, through its Contracted HIE Vendor, will store and update a master patient index to locate patient records in the System. The master patient index will be configured to match patient records submitted by Participants based on pre-defined rules and algorithms using demographic data. WISHIN will develop a process to detect and notify Participants of potential duplicates or non-matching records that may be the same patient. WISHIN will provide this information to Participants, to allow them to determine whether they will correct the records in their systems to resolve those issues.

If a Participant notices duplicate patients/non-matching patient records in the master patient index, the Participant will take the following steps:

- If the disparity is among the Participant's own records, then the Participant will correct its records to resolve the issue.
- If the disparity is among records contributed by multiple Participants, the Participant will notify WISHIN about the disparity. WISHIN will assist Participants in resolving duplicate/unmatched patients; however, WISHIN will not modify any information in the Participant's data submitted to the System.

WISHIN may temporarily link patients together in the master patient index until a duplicate/non-match is resolved in the Participants' source records.

Policy 1300: Amendment of Privacy Policies

ONC Domain: Accountabilty

Scope and Applicability: This Policy applies to WISHIN, all Participants and their Business Associates and contractors.

Policy:

The procedures described in this policy do not apply to non-substantive, clarifying changes to WISHIN's policies or to changes required to make corrections to WISHIN's policies.

Privacy Policy Review

WISHIN will review these Privacy Policies periodically as changes in applicable laws and circumstances may warrant, or at a minimum, annually.

A Participant can request that WISHIN conduct a review of its Privacy Policies by submitting a request to WISHIN. The request must contain:

- The policy(ies) that should be reviewed
- The reason(s) a review is necessary
- The requested timeframe for the review

Upon its receipt of such request, WISHIN will cooperate with the requesting Participant in determining whether a special review is necessary or whether the request can be part of the annual review.

Privacy Policy Amendments

Approval of Amendments

If WISHIN determines, upon review, that amendments to the Privacy Policies may be necessary, WISHIN will draft proposed amendments and present the amendments for approval as described below.

Amendments to WISHIN Privacy Policies are subject to approval of the WISHIN Board of Directors and the Participant Advisory Board.

Amendments to Privacy Policies shall be approved by the Participant Advisory Board before being presented to the Board of Directors.

"Participant Advisory Board" means the advisory board of System participants having the following representation:

- Rural/CAH hospital representative,
- Independent hospital representative (non-system, non- CAH),
- Independent-clinic representative,
- Five Milwaukee health-system representatives, for so long as each remains a System participant:
  - Aurora Health Care, Inc.
  - Children's Hospital and Health System, Inc.
  - Columbia St. Mary's, Inc.
  - Froedtert Health, Inc.

  - Wheaton Franciscan Services, Inc.
- Two non-Milwaukee health system representatives,
- Milwaukee Health Care Partnership representative, and
- State of Wisconsin Department of Health Services representative

No other categories of Other Participants shall be represented on the Participant Advisory Board unless approved by the WISHIN Board of Directors and Participant Advisory Board.

Material Changes to Privacy Policies

Any "material change" in Privacy Policies that is approved by the Participant Advisory Board and the Board of Directors will include a determination whether it is technically feasible and financially reasonable for WISHIN to allow a Participant to opt out of participating in the change while still remaining a System Participant. "Material change" includes any change that materially reduces, limits, or modifies the functionality or levels of service provided, or any change in the Permitted Purposes or the List of Eligible Participants, as stated in the participation agreement.

Publication and Notice to Participants of Amendments to Privacy Policies

After amendments to Privacy Policies have been approved by the Participant Advisory Board and the WISHIN Board of Directors, WISHIN shall publish the amendments on its website at www.wishin.org and notify Participants of amendments prior to the effective date of the amendment (following posting requirements in the Participation Agreement).

The notification will include:

- A list of the policies that have been amended, the details of each amendment, and reasons for each amendment
- The effective dates of the amendments
- If applicable, the timeframe within which Participants must respond to Privacy Policy Amendments, along with instructions on how to respond.

If an amendment constitutes a "material change" in Privacy Policies, the notice shall also include all of the following:

- A determination whether it is technically feasible and financially reasonable for Participant to opt out of the change while still being a System participant
- Instructions as to what Participants must do to opt out, and
- The deadline for opting out.

Agreement to Comply Upon Effective Date

Participants agree to comply with an amendment to the Privacy Policies as of the effective date of the amendment.

If Participants do not complete instructions for opting out of a "material change" by the date specified in the notice to Participants, WISHIN will deem their silence as consent to any proposed policy amendments and agreement to comply with the new policies on their effective date.

Participants' Right to Withdraw From the System

If Participant is unable or unwilling to comply with such Policies and Procedures, Participant may elect to suspend its use of the System or terminate its Data Sharing Participation Agreement pursuant to the terms of its Participation Agreement.

Effect of Policy Amendment on Prior Versions

An amended Privacy Policy replaces any prior versions of the policy as of its effective date.