WISHIN

Wisconsin Statewide Health Information Network

2012

Privacy Policies

Contents

Introduction

The following policies apply to the access, use, and disclosure of protected health information by Participants through the services being made available to Participants by WISHIN. These services are collectively referred to as the "System." It is anticipated these policies will be reviewed and revised as needed based on the experience of WISHIN, the Participants, and the input provided by WISHIN's advisory committees.

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 consumer control of and access to health information and the operational need of covered entities to ensure that information uses and disclosures are not overly restricted, such that consumers 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 information will help decrease the amount of privacy violations, which may occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

[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

Disclosure Limitation

Personal 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 decision and the potential disadvantages. (ONC Domain(s): 5 - Collection, Use, and Disclosure Limitation)

Access and Use Limitation

Personal health information should be obtained by one Participant from another only pursuant to mutual agreement that the information is being accessed for qualifying treatment or payment purposes of the requesting Participant. Information recipients may use and disclose protected health information obtained through the System only for purposes and uses consistent with their permitted access and consistent with their obligations as covered entities under HIPAA. Certain exceptions, such as for law enforcement or public health, may warrant reuse of information for other purposes. However, when information obtained by a Participant through the System is used for purposes other than those for which the information was originally obtained, the Participant so using or disclosing the information should first apply the rules applicable to it as a covered entity under HIPAA and as a contracting Participant. (ONC Domain(s): 5 - Collection, Use, and Disclosure Limitation)

Individual Participation and Control

Consistent with the scope of individual rights in HIPAA, individuals should have the right to request and receive in a timely and intelligible manner information regarding various parties that may have that individual's specific health information; to know any reason for a denial of such request; to request to amend any protected health information that the individual believes is inaccurate; and to request not to have his or her information made available through the System. Individuals have a vital stake in personal protected health information, such rights enable individuals to make informed decisions about participation and 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 protected health information and individuals must be allowed to view information about them 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. (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, such as those who will provide data to the System, are unlikely to fully trust the System and fully participate, if they believe other Participants are not applying the same rules and being held to the same standard of accountability. 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

To ensure privacy protection there must be legal and financial remedies that hold violators accountable for failing to comply with System policies. Such remedies will give individuals confidence in the organization'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 Covered Entity 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. WISHIN should identify, disseminate and enforce only those policies and procedures necessary for coordination of privacy response, but should recognize 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 outlines in the ten principles as well as basic requirements set forth in HIPAA. 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

Participants – those which provide data to the System and those which obtain and use data from the System – are health care providers, health plans, or health care clearinghouses. 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 ("BA") 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 P.L 111-5 and regulations to be issued thereunder.

WISHIN policies and the health information technology design components and safeguards need to be developed in accordance with Wisconsin Statute Chapter 51.30, which contains special provisions regarding release of alcohol, drug abuse, developmental disabilities and mental health records.

Safeguards in an Electronic Networked 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 operations and for the purposes of treatment, payment, and operations *of such third parties, without written authorization.*[1] HIPAA limits authority to disclose without authorization in other situations and attaches conditions. 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 or payment 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 RLS 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, WISHIN and Participants have placed the burden on the requesting Participant to:

- Access information from another Participant's records only for a qualifying treatment or payment use by the requesting Participant. A qualifying treatment or payment use is one that would permit the Participant from whose records the information is accessed to disclose such information to the requesting Participant under §§164.506(c)(2) and (3) of the Privacy Rule.

[1] 45 C.F.R. §§164.506(c)(3) and (4).

- In connection with access for payment purposes, to access and use only the minimum information necessary for purposes of the payment needs of the Participant accessing the information.

To support this approach, WISHIN and the Participants have implemented the following administrative safeguards:

All Participants must be covered entities under HIPAA and therefore individually subject to regulation and penalties.

1. All Participants commit to accessing PHI only for the purposes of their treatment, payment, and operations. While §164.506(c)(4) permits limited disclosure for the health care operations of another Participant, the System is only to be used by Participants to access protected health information for the purposes their of treatment, payment, and operations.
2. Participants that are providers may request PHI from other Participants only for their treatment or payment purposes.
3. Participants that are health plans may request PHI from other Participants only for their payment purposes.
4. Participants that are acting as plan administrator of health plans covered under HIPAA may request PHI from other Participants only in connection with payment activities of the plans they administer.
5. "Treatment" and "payment," as used in these policies and explanations, have the meaning given in Section §164.501 of the Privacy Rule.

WISHIN and all Participants are subject to the additional regulations and penalties in Wisconsin Statute Section 51.30, which deals with restrictions on release of records related to alcohol, drug abuse, developmental disabilities, and mental health.

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 to ensure compliance.[2]

Each Participant shall itself be a HIPAA "covered entity" or "business associate" and 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.

WISHIN Policies

Each Participant shall, at all times, comply with these WISHIN Policies ("WISHIN Policies"). These WISHIN Policies may be changed and updated from time to time upon reasonable written notice to Participants. Amendment shall be effective when adopted by the WISHIN Board of Directors, ordinarily following input by WISHIN's advisory committees and workgroups. WISHIN shall notify Participants of all policy changes. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these WISHIN Policies.

Participant Policies

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

User Criteria

Authorized users are individuals who have been granted access authority. 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 BA or workforce of such BA, or (iii) an individual contractor or subcontractor of a BA or workforce of such contractor or subcontractor. Additionally, a Participant that is a covered health plan may also be an authorized user in its role as a third party administrator and BA for self-funded group health plans that are covered entities under HIPAA but are not themselves Participants.

[2] 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.

Application to WISHIN Employees

WISHIN will ensure that its employees, contractors, and business associates 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 establishing certain individual privacy rights.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate 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 ensure openness and transparency, Participants who are health care providers shall 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[3] 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 operations; and to public health entities as required 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 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, [4] 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.

[3] 45 C.F.R. §§ 164.520(b).

[4] 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 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. WISHIN will maintain an individual's election to opt out, described below, as part of the master patient information.

Individual's Choice to Have Information Available

Individuals will have the opportunity to opt out of having their health information viewable by participants in the System. Participants will send all of the required health information to the System (including the information of individuals who opt out), and if an individual has elected to opt out, that individual's health information will not be available to other participants in the System.

Participants agree to provide the opportunity for individuals to elect to opt out, subject to qualifications and limitations described in the informational brochure referred to below or in these policies. That is, a request shall not be accepted to the extent it agrees to restrictions that exceed the then current physical, technical and administrative capabilities of the System.

1. Individuals shall be afforded the opportunity to exercise this choice at the time of any service at a Participant that is a health care provider or thereafter through a uniform "opt-out" process.
2. 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. Participants may customize the informational brochure as they deem appropriate to fit their circumstances. 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.
3. 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 from being part of the exchange as prohibited by federal and state law. The brochure will explain that a Participant's policies continue to govern access, use, and disclosure in all other contexts.
4. 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 and Immunization Registry reporting, as required by law.

5. 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.
6. Participants should furnish the brochure to individuals at the initiation of an episode of care and note for individuals the opportunity to opt-out or ask questions. Each Participant will have one or more persons designated to answer questions about the System or about opting out or revoking a prior opt-out election.
7. 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.
8. Participants that are health plans provide only limited enrollment and eligibility information through the System and have limited or no face-to-face contact with individuals. Participants that are health plans shall provide a description of the System, an explanation of the right to opt out, a link to the WISHIN website, and a phone number individuals can use to obtain additional information about the System, insurer access, and the right to opt out in their privacy communications to individuals and otherwise as they determine necessary.
9. An individual's election to opt out of participation in the System shall be communicated to WISHIN in the manner provided by WISHIN and be of System-wide effect once so communicated and processed.

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 withdrawing 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 communicated through the System.

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.

Documentation

Each Participant shall document and maintain documentation that information about the System and about the ability to opt out of the System has been provided to the Participant.

Participant'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.

Provision of Coverage or Care

A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice to opt out.

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).

Policy 400: Access to and 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 and disclose 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 protected health information for a particular purpose, the disclosing institution shall ensure that it has obtained the required documentation or met the requisite conditions. Each disclosure, access, and use of protected health information by a Participant is a representation to every other Participant in the System that the health information being disclosed, accessed, or used has met all prerequisites under state and federal law for such disclosure, access, or use.[5]

Purposes

A Participant may request and use protected health information through the System only for the purposes of Participant's treatment, payment, and operations, and only to the extent necessary and permitted by applicable federal, state, and local laws and regulations and these Policies.[6] 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.

Prohibitions

Information may not be requested for fundraising, marketing or purposes related to fundraising or marketing without specific patient authorization. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request or access information through the System.

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 minimum necessarry.[7]

[5] 45 C.F.R. § 164.530(j).

[6] 45 C.F.R. § 164.502(a), (b).

[7] 45 C.F.R. § 164.502(b).

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 record and thereafter use and disclose the merged information only in a manner consistent with its own information privacy policies and laws and regulations applicable to its own record. 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 Participant's qualifying treatment, payment, and operations purposes.

Disclosures to Law Enforcement

If a law enforcement official requests PHI from WISHIN via a court order, subpoena, warrant, summons, or other similar document, 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 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. 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. To alert law enforcement of the death of the individual;
4. If WISHIN believes the PHI requested constitutes evidence of criminal conduct that occurred on the premises of WISHIN;
5. 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;
6. It is aggregate data that could not be easily obtained by a law enforcement request to individual Participant(s);
7. It is information stored only by WISHIN, such as audit logs or reports of access to information;

and:

1. If the PHI sought is relevant and material to the law enforcement inquiry;
2. The request is specific and limited in scope to the extent reasonably practicable;
3. De-identified PHI could not be used; and
4. The court order, subpoena, warrant, summons, or other similar document complies with Wisconsin law which in some cases requires patient authorization to release.

If a WISHIN employee is presented with a court order, subpoena, warrant, summons, or other similar document, the employee will immediately notify the Privacy Officer and/or WISHIN legal counsel of the document who will evaluate the document and determine whether and how the disclosure will be made. No PHI will be disclosed in response to a court order, subpoena, warrant, summons, or

other similar document prior to discussing the document with the Privacy Officer and/or legal counsel.

The person providing PHI in response to a court order, subpoena, warrant, summons, or other similar document 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, and 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.[8] Unless a Participant requesting information notes otherwise: (i) each request by a Participant that is a provider is deemed to be for such Participant's treatment purposes, (ii) each request by a Participant that is a health plan is deemed to be for such Participant's payment purposes, and (iii) each request by a Participant that is acting as a plan administrator of one or more other health plans covered by HIPAA is deemed to be for the payment purposes of such other health plans. 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.

[8] 45 C.F.R. § 164.528. For HIPAA Covered Entities, this is currently required by law.

Audit Logs

Participants and WISHIN shall develop an audit log capability to document which Participants posted and accessed the information about an individual through the System and when such information was posted and accessed.[9] 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.[10, 11] 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.

Access

Each Participant should have a formal process through which it permits individuals to view information about them that has been posted by the Participant to the System.[12] Participants and WISHIN shall consider and work towards providing patients direct access to the information about them contained in the System.[13] This capability will not be available at the WISHIN launch date.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

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

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

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

[12] See 45 C.F.R. § 164.524.

[13] See **Connecting for Health**, "Patients' Access to Their Own Health Information."

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

The System and these policies are geared to the HIPAA level of privacy. Some health information may be subject to special protection under federal, state, and/or local laws and regulations, including Wisconsin Statute Section 51.30, covering records relating to alcohol and drug abuse, developmental disabilities, and mental health. Other health information may be deemed so sensitive that a Participant has made special provision to safeguard the information, even if not legally required to do so.

Each Participant shall be responsible to identify what information is legally subject to special protection under applicable law and what information (if any) is subject to special protection under that Participant's policies, prior to disclosing any information through WISHIN. Participants should not make protected health information requiring special protection available to the System. Each Participant is responsible for complying with laws and regulations and its own policies in regard to identifying and providing special treatment for information needing special protection.

Information Not Furnished

Participants accessing and using another Participant's information obtained through the System should assume that the information made available would not include any of the following:

1. Alcohol and substance abuse treatment program records;[3]
2. Developmental disability treatment records; [4]
3. Mental health treatment records; [5]
4. Records of emergency protective custody proceedings; [6]
5. Records of predictive genetic testing performed for genetic counseling purposes;[7]

This list is suggestive only. Other records may be added to the list. Data recipients are not entitled to rely on records being inclusive of the above listed records.

[3] Wisconsin Statute §51.30(4)(a)

[4] Wisconsin Statute §51.30(4)(a)

[5] Wisconsin Statute §51.30(4)(a)

[6] Wisconsin Statute §51.30(4)(a) and Wisconsin Statute §55.22

[7] There is pending Wisconsin legislation that may require these records to be excluded from the System

Application to Business Associates and Contractors

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate 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 BAs 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.

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

A Participant that is a health plan shall access and use PHI of another Participant only for "payment" purposes as defined in 42 C.F.R. § 164.501. Participants that are health plans shall initiate a search through the System only: (i) to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; (ii) to obtain or provide reimbursement for the provision of health care; (iii) to determine eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (iv) to risk adjust amounts due based on enrollee health status and demographic characteristics; (v) for billing, claims management, collection activities, obtaining payment under a contract for reinsurance, including stop-loss insurance and excess of loss insurance, and related health care data processing; (vi) to review health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and (vii) for utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services. All Participants shall access and use only the minimum information necessary when accessing and using information for payment purposes. A Participant that is a health plan shall not access protected health information related to a specific encounter and/or treatment of a patient if the patient has paid the health care provider directly out of pocket in full for such encounter and/or treatment.

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 BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

Policy 700: Workforce, Agents, and Contractors

ONC Domain: Collection, Use and Disclosure Limitation
Safeguards
Accountability

Scope and Applicability: This Policy applies to WISHIN and all Participants and their BAs 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

All authorized users, whether members of a Participant's workforce or member of the workforce of a BA or contractor, shall execute an individual user agreement and 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, BA, or contractor, as applicable. Participants shall determine to what extent members of their workforce or the workforce of BAs and contractor require additional training on account of the Participant's obligations under their participation agreement and these policies, 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.

Discipline for Non-Compliance

Each Participant shall implement procedures to discipline and hold authorized users, BAs and contractors accountable for following the Participant's policies and procedures and for ensuring that

they do not use, disclose, or request health information except as permitted by these Policies.[15] Such discipline measures may include, but not be limited to, verbal and written warnings, demotion, and termination and may provide for retraining where appropriate.

Reporting of Non-Compliance

Each Participant shall have a procedure, and shall encourage all workforce members, BAs and contractors to report any non-compliance with the Participant's policies or the policies applicable to authorized users.[16] 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 BAAs and Contractor Agreements

Each Participant shall require in any relationship with a BAs, 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 when accessing, using or disclosing information through the System; (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; and (iii) that such third party may have its contract with the Participant terminated for violation of these Policies or for failure to enforce these policies among its workforce.

[15] 45 C.R.F. § 164.530(e).

[16] 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.[17] 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 BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

[17] 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,[18] as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions. This shall include not making the individual's information available to the System, including opting the individual out of the System, if required by the restriction. Participants should advise individuals that opting out only affects access, use and disclosure of their protected health information through the System. 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.

[18] 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 BAs and contractors.

Policy:

Individual Complaints

Any individual may submit a complaint about an access, use, or disclosure of PHI by WISHIN to either WISHIN or to 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 implicating privacy or security safeguards deployed by WISHIN (or its contractors) according to its own policies. 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. Any other steps mutually agreed to as appropriate under the circumstances; and
7. Any other step 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 and/or individual complaints filed with 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.

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

Duty to Cooperate 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 BAs 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 BAs and to the contractors and subcontractors of their BAs as they deem appropriate 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 business associate of WISHIN, the HIPAA Privacy Officer will notify the business associate of the results of the investigation and any required action on the part of the business associate. If the results of the investigation are that the WISHIN business associate 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 business associate relationship between the business associate 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 sanctions, 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 BAs and contractors. This Policy is to be read and applied in conjunction with the WISHIN Security Policy.

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 BAs 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 BA or contractor to train and supervise its authorized users consistent with the Participant's and WISHIN's privacy policies and with the terms of the Participant's privacy policies and the BA Agreement 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. Hold their authorized users accountable for compliance with WISHIN and the Participant's policies and, as applicable, the terms of any BA Agreement.

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 BA 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 ensure 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 BA 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 contractor.
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 BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.