

HIE Architectural Model: Point-to-Point Directed Exchange

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing (if needed, use additional documents to describe and insert reference here)
Required to address			
Openness and Transparency	<p>Not applicable for WISHIN for point-to-point directed exchange. WISHIN itself does not access individually identifiable health information (IIHI) or use IIHI beyond what is required to encrypt and route the information. WISHIN does not know what information exists about a patient, how it was collected, how it is used or disclosed.</p> <p>WISHIN uses the Direct standards established by the National Direct Project, therefore, the content of the messages sent via WISHIN Direct cannot be accessed by WISHIN. Without knowledge of the content of the message(s), WISHIN has no information on what was exchanged related to an individual's health information.</p> <p>Participants, by signing the Direct+ Participation Agreement, agree to comply with all applicable federal and state laws, including HIPAA, regarding disclosure of data practices.</p>	<p>Not applicable; however, the WISHIN website (www.wishin.org) provides a significant amount of information on WISHIN Direct+ that is publicly available.</p>	n/a
Collection, Use and Disclosure Limitation	<p>Participants must sign a Participation Agreement, with an accompanying Business Associate Agreement, which contains the following provision:</p>	<p>The WISHIN Direct+ Participation Agreement requires a signature by any participant prior to receiving a Direct address with WISHIN Direct+.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>3.d. Minimum Necessary. In its performance of the functions, activities, services, and operations specified above, Business Associate will make reasonable efforts to use, disclose, and request only the minimum amount of Participant’s Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that Business Associate will not be obligated to comply with this minimum-necessary limitation if neither Business Associate nor Participant is required to limit its use, disclosure or request to the minimum necessary. To the extent it uses, discloses, and requests PHI in a manner that involves Business Associate, Participant will make reasonable efforts to use, disclose, and request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request to the extent it is required to do so under HIPAA. The phrase “minimum necessary” shall be interpreted in accordance with the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), passed as part of the American Recovery and Reinvestment Act of 2009, and HHS guidance.</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing (if needed, use additional documents to describe and insert reference here)
Safeguards	<p>WISHIN authenticates all participants before they are given a Direct+ and authorized to use the WISHIN Direct+ system.</p> <p>WISHIN Direct+ is encrypted using Payload data encrypted using randomly generated 2048-bit AES symmetric keys.</p> <p>Prior to being authorized to use the system, Participants must sign a Participation Agreement, with an accompanying Business Associate Agreement, which contains the following safeguard provision:</p> <p>5. Safeguards Against Misuse of Information. Business Associate will develop and use appropriate administrative, technical and physical safeguards to prevent the improper use or disclosure of PHI. Such safeguards shall include, but not be limited to, developing, documenting and keeping current policies and procedures and training personnel regarding the proper use and disclosure of PHI. If Business Associate creates, receives, maintains or transmits EPHI on behalf of Participant, Business Associate shall implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and</p>	<p>The WISHIN Direct+ Participation Agreement requires a signature by any participant prior to receiving a Direct address with WISHIN Direct+.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>availability of Participant's EPHI as required by the Security Rule. Such safeguards shall include, but not be limited to, developing, implementing and maintaining adequate: administrative safeguards to manage the selection, development, implementation, and maintenance of security measures to protect EPHI; physical safeguards to protect Participant's EPHI from natural and environmental hazards, and unauthorized intrusion; and technical safeguards for its use that protect EPHI and control access to such information.</p>		
Accountability	<p>Prior to being authorized to use the system, Participants must sign a Participation Agreement, with an accompanying Business Associate Agreement, which contains the following provisions:</p> <p>7. Reporting of Any Breach, Improper Use or Disclosure, and Security Incidents.</p> <p>a. Breach. Business Associate shall notify Participant without unreasonable delay (and in no case later than 60 days after discovery of a Breach) of any Breach of Unsecured Protected Health Information. The notice shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is</p>	<p>The WISHIN Direct+ Participation Agreement requires a signature by any participant prior to receiving a Direct address with WISHIN Direct+.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. Business Associate shall provide Participant with any other available information that Participant is required to include in notification to the individual under 45 C.F.R. § 164.404(c) at the time Business Associate provides notification of any Breach or promptly thereafter as information becomes available.</p> <p>b. Security Incidents. Business Associate will report to Participant any Security Incident of which Business Associate becomes aware.</p> <p>c. Other Improper Uses and Disclosures. Business Associate shall report to Participant any use or disclosure of Participant’s PHI that is not provided for by this Exhibit of which Business Associate becomes aware.</p> <p>10. Accounting of Disclosures. Business Associate agrees to make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528.</p> <p>11. Availability of Books and Records. Business Associate will</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Participant available to the Secretary of the United States Department of Health and Human Services for purposes of determining Participant's compliance with the Privacy Rule.</p>		
Optional to address			
Individual Access	<p>Not applicable for WISHIN for point-to-point directed change. WISHIN itself does not access IIHI or use IIHI beyond what is required to encrypt and route the information. WISHIN does not know what information exists about a patient, how it was collected, how it is used or disclosed.</p> <p>WISHIN uses the Direct standards established by the National Direct Project, therefore, the content of the messages sent via WISHIN Direct cannot be accessed by WISHIN. Without knowledge of the content of the message(s), WISHIN has no information on what was exchanged related to an individual's health information.</p> <p>If requested by an individual for a copy of his/her IIHI, WISHIN will direct the individual to work directly with his/her health care providers.</p>	n/a	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing (if needed, use additional documents to describe and insert reference here)
Correction	<p>Prior to being authorized to use the system, Participants must sign a Participation Agreement, with an accompanying Business Associate Agreement, which contains the following provision:</p> <p>9. Amendments to PHI. If PHI is in a Designated Records Set, Business Associate agrees to make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526.</p>	<p>The WISHIN Direct+ Participation Agreement requires a signature by any participant prior to receiving a Direct address with WISHIN Direct+.</p>	n/a
Individual Choice	<p>Not applicable for WISHIN for point-to-point directed change. WISHIN itself does not access IIHI or use IIHI beyond what is required to encrypt and route the information. WISHIN does not know what information exists about a patient, how it was collected, how it is used or disclosed.</p> <p>WISHIN uses the Direct standards established by the National Direct Project, therefore, the content of the messages sent via WISHIN Direct cannot be accessed by WISHIN. Without knowledge of the content of the message(s), WISHIN has no information on what was exchanged related to an individual's health information.</p>	n/a	n/a
Data Quality and Integrity	<p>Not applicable for WISHIN for point-to-point directed change. WISHIN itself does not access IIHI or use IIHI</p>	<p>The WISHIN Direct+ Participation Agreement requires a signature by any participant prior to receiving a</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>beyond what is required to encrypt and route the information. WISHIN does not know what information exists about a patient, how it was collected, how it is used or disclosed.</p> <p>WISHIN uses the Direct standards established by the National Direct Project, therefore, the content of the messages sent via WISHIN Direct cannot be accessed by WISHIN. Without knowledge of the content of the message(s), WISHIN has no information on what was exchanged related to an individual's health information. Therefore, the following language is in the General Terms and Conditions of the Participation Agreement between WISHIN and participants of WISHIN Direct+</p> <p>a. Accuracy of Patient Record Matching. Participant acknowledges that there could be errors or mismatches when matching patient identities between disparate data sources, but WISHIN shall take commercially reasonable measures to help ensure accurate patient matching occurs, if WISHIN is involved in matching for the particular service to which Participant is subscribed. Participant is solely responsible for ensuring that any PHI obtained</p>	<p>Direct address with WISHIN Direct+.</p>	

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>through the Network relates to a particular individual as intended by Participant and for the immediate destruction of any PHI obtained inadvertently.</p> <p>b. Accuracy of Health Data. Nothing in these Terms and Conditions shall be deemed to impose responsibility or liability on Participant or WISHIN related to the clinical accuracy, content or completeness of any Health Data provided pursuant to these Terms and Conditions.</p>		

HIE Architectural Model: Data Aggregation

(HIE entities that store, assemble or aggregate individually identifiable health information, whether centrally or in a federated model)

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
Required to address			
Individual Access	<p>WISHIN Policies: Policy 300: Individual Control of Information Available 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 aide the individual in obtaining the information from Participants.</p> <p>WISHIN Practices: WISHIN will assist individuals in identifying sources of their individually identifiable health information. However, WISHIN will direct individuals to the sources of the information, so they can request copies of that information from those sources.</p>	<p>Privacy Policies are published on WISHIN's website, which is available to the public.</p> <p>Privacy Policies are also made part of the data sharing agreement between participants and WISHIN; participants agree to abide by WISHIN's privacy policies by means of their signature on the data sharing agreement.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
Correction	<p>WISHIN Policies:</p> <p>Policy 800: Amendment of Data – Each Participant shall comply with applicable federal, state, and local laws and regulations regarding individual rights to request amendment of health information. 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.</p> <p>WISHIN Practices: Because correction of data should be done at the source of information, WISHIN will assist participants and individuals in identifying any information that in the HIE about the individual, but Participants will correct data in their own systems. The WISHIN HIE will accept data correction transactions submitted by Participants</p>	<p>Privacy Policies are published on WISHIN’s website, which is available to the public.</p> <p>Privacy Policies are also made part of the data sharing agreement between participants and WISHIN; participants agree to abide by WISHIN’s privacy policies by means of their signature on the data sharing agreement.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
Openness and Transparency	<p>WISHIN Policies:</p> <p>Policy 200: Notice of Privacy Practices – Participants 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.</p> <p>Policy 300: Individual Control of Information Available Through the System – WISHIN furnish Participants 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.</p> <p>WISHIN Practices:</p> <p>WISHIN has developed materials participants will deliver to individuals, informing them about the WISHIN HIE, the types of data being exchanged, and their choice to opt out of having their information available to other providers. WISHIN has also developed posters for participants to display at</p>	<p>Privacy Policies are published on WISHIN’s website, which is available to the public.</p> <p>Privacy Policies are also made part of the data sharing agreement between participants and WISHIN; participants agree to abide by WISHIN’s privacy policies by means of their signature on the data sharing agreement.</p> <p>Participants will distribute patient choice brochures to individuals when they are provided with care. Patient choice brochures are also available to individuals through WISHIN’s website.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>their facilities, informing individuals about the WISHIN HIE.</p> <p>WISHIN had the patient materials reviewed by focus groups to ensure the brochure language was simple, understandable, and at an appropriate literacy level. The materials are available in multiple languages.</p> <p>WISHIN HIE contains audit log reports that participants run to get an log of everyone who has accessed an individual's record in the HIE, which can be provided to an individual upon the individual's request.</p>		
Individual Choice	<p>WISHIN Policies:</p> <p>Policy 300: Individual Control of Information Available Through the System – Individuals will have the opportunity to opt out of having their health information viewable by Participants. 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, except in the limited circumstances described below.</p> <p>Participants agree to provide the opportunity for individuals to elect to opt out, subject to qualifications and limitations described in the</p>	<p>Privacy Policies are published on WISHIN's website, which is available to the public.</p> <p>Privacy Policies are also made part of the data sharing agreement between participants and WISHIN; participants agree to abide by WISHIN's privacy policies by means of their signature on the data sharing agreement.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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.</p> <ol style="list-style-type: none"> 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 furnish Participants 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. 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 		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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.</p> <p>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. An individual's health information may also be accessed if specific consent is given by the individual to a provider or in an emergency situation where health information is necessary for treatment and the individual is unable to give consent.</p> <p>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.</p> <p>6. Participants should furnish the brochure to individuals at the initiation of an episode of care and</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>inform individuals of 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.</p> <p>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.</p> <p>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 to individuals, as</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>required by law and otherwise as they determine necessary.</p> <p>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.</p> <p>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.</p> <p>Policy 900: Requests for Restrictions – If a Participant agrees to an individual's request for restrictions 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, 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</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>agreeing to the restriction would have on the accuracy, integrity and availability of information through the System.</p> <p>WISHIN Practices: WISHIN has developed materials participants will deliver to individuals, informing individuals about the WISHIN HIE, the types of data being exchanged, and their choice to opt out of having their information available to other providers. The same form can be used by individuals to revoke their previous opt-out decision, if desired. The opt-out materials are also available to individuals on WISHIN's website.</p> <p>WISHIN had the patient materials reviewed by focus groups to ensure that the information in the brochures was simple, understandable, and at an appropriate literacy level. The materials are available in multiple languages.</p>		
Collection, Use and Disclosure Limitation	<p>WISHIN Policies: Policy 100: Compliance with Law and Policies – Participants agree to apply with all applicable federal, state, and local laws and regulations, including HIPAA. Even participants that are not “covered entities” under HIPAA agree to comply with HIPAA</p>	<p>Privacy Policies are published on WISHIN's website, which is available to the public.</p> <p>Privacy Policies are also made part of the data sharing agreement between participants and WISHIN; participants agree to abide by WISHIN's privacy policies by means of their signature on</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>privacy and security requirements relating to the protection, disclosure, and use of PHI, as if they were “covered entities.”</p> <p>Participants also agree to comply with WISHIN Privacy Policies related to data use and access.</p> <p>Policy 400: Access to, Use, and Disclosure of Information –</p> <p>Participants will access, use, disclose, and/or dispose of PHI in a manner consistent with all applicable federal, stat, and local laws and regulations. Participants are required to obtain the appropriate consents required or disclosing or accessing specially protected information.</p> <p>Participants may use PHI only to the extent necessary and permitted under applicable laws. Participants may request and use PHI only if the participant has, has had, or is about to have the requisite relationship to the individual whose PHI is being accessed and used.</p> <p>Participants are prohibited from using patient information for fundraising, marketing, or purposes related thereto, without specific patient authorization. Information may not be requested for a discriminatory purpose. Participants may not request</p>	<p>the data sharing agreement.</p>	

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>or access information in the absence of a permissible purpose.</p> <p>Policy 500: Information Subject to Special Protection – Participants must comply with Wis. Stat. Sec. 51.30, meaning they must obtain prior patient written consent if requesting/disclosing records covered under that statute; or attest that the patient was unable to give such consent in an emergency situation and the PHI is necessary for treatment.</p> <p>Policy 600: Minimum Necessary – Each participant will only request/access a patients data for treatment purposes, or the minimum amount of health information necessary for the intended purpose of the request. Health plans are only to use PHI for payment purposes defined in 42 CFR 164.501.</p> <p>Policy 700: Workforce, Business Associates, and Contractors – Participants will allow access to the System only by those authorized uses who have a legitimate and appropriate need to use the system. Any business associate, contractor or other third party that is a user of the system on behalf of Participant is required to comply with WISHIN’s Privacy Policies. Participants shall have procedures for reporting and taking corrective actions for any system</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>users who do not comply with WISHIN Privacy Policies.</p> <p>WISHIN Practices: WISHIN has safeguards in its system to determine whether participants have a relationship with patients before allowing a user to access a patient's information. If the user wants to establish a relationship, that information is logged in WISHIN's audit log, which is available to participants for auditing.</p> <p>WISHIN also requires users who attempt to access data protected under Wis. Stat. 51.30 to attest they have obtained the appropriate consent or that it is an emergency situation and the patient is unable to provide consent, provide a reason for accessing the information, and produce the consent upon request by WISHIN or the disclosing participant. All access to this type of information.</p>		
Data Quality and Integrity	<p>WISHIN Policies: Policy 800: Amendment of Data – Each Participant shall comply with applicable federal, state, and local laws and regulations regarding individual rights to request amendment of health information. If an individual requests, and the Participant accepts, an amendment to the health</p>	<p>Privacy Policies are published on WISHIN's website, which is available to the public.</p> <p>Privacy Policies are also made part of the data sharing agreement between participants and WISHIN; participants agree to abide by WISHIN's privacy policies by means of their signature on the data sharing agreement.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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.</p> <p>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.</p> <p>Policy 1200: Ownership and Modification of Data in the System – Each Participant shall remain the owner of the data it makes available for the System, and each Participant shall be responsible for the quality and integrity of the data it contributes to the system.</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>WISHIN shall not modify any data in the System owned by Participants. However, WISHIN may:</p> <ul style="list-style-type: none"> • 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 <p>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.</p> <p>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. Participants will correct the records in their systems to resolve those issues.</p> <p>If a Participant notices duplicate patients/non-matching patient records</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>in the master patient index, the Participant will take the following steps:</p> <ul style="list-style-type: none"> • 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. <p>WISHIN may temporarily link patients together in the master patient index until a duplicate/non-match is resolved in the Participants’ source records.</p> <p>WISHIN Practices:</p> <p>WISHIN’s HIE contains matching functions for both single data sources and across the HIE. The matching is done based on defined rules related to demographic information and phonetic algorithms. The system can use up to 27 different pieces of demographic information to determine matches, along with some enhanced matching based on factors such as “fuzzy” dates and common nicknames. Each participant develops its own matching</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>specifications for its own data feeds, which are then incorporated into the HIE master patient matching specifications. WISHIN considers anything that matches with a 95% degree of confidence or higher in the matching logic algorithms to be a potential match.</p> <p>The system accepts HL7 patient merge/move transactions to keep matching up to date with participants' EHR corrections.</p> <p>WISHIN will assist participants in identifying any potential patient matches or incorrect matches, and help facilitate correction of data in affected Participants' EHRs. If data correction cannot be done for some reason or another to achieve proper matches, WISHIN will use its own web tool to link or separate patient records, as appropriate.</p>		
Safeguards	<p>Policy 700: Workforce, Business Associates, and Contractors – 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.</p> <p>Each Participant is responsible to establish and enforce policies designed to comply with its</p>	<p>Privacy Policies are published on WISHIN's website, which is available to the public.</p> <p>Privacy Policies are also made part of the data sharing agreement between participants and WISHIN; participants agree to abide by WISHIN's privacy policies by means of their signature on the data sharing agreement.</p> <p>WISHIN Security Policies are</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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. 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. 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. 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. Each Participant shall require in any relationship with a Business Associate, contractor, or other third</p>	<p>published on WISHIN's website, which is available to the public, and will also be furnished to any participant upon request.</p> <p>WISHIN Participant Safeguard Checklist is presented to participants during the onboarding process.</p>	

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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.</p> <p>Policy 1000: Privacy Breaches – Investigations and Mitigation – 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</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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. 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</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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.</p> <p>Policy 1100: Authorized User Controls – Each Participant is responsible to:</p> <ol style="list-style-type: none"> 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 and WISHIN's privacy policies, the Business Associate Agreement, and 		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>all applicable state and federal laws, as applicable.</p> <p>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.</p> <p>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.</p> <p>6. Hold their authorized users accountable for compliance with WISHIN and the Participant's policies and, as applicable, the terms of any Business Associate Agreement.</p> <p>WISHIN is responsible to:</p> <p>1. Grant access authority to individuals designated by a Participant, subject</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>to reserved authority to suspend, limit, or revoke such access authority as described later.</p> <ol style="list-style-type: none"> 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 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 		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>user agreement, if WISHIN determines that doing so is necessary for the privacy of individuals or the security of the System.</p> <p>Security Policy Document: WISHIN has developed a system security policy document which includes information stewardship, privacy and security governance, risk analysis and management, sanctions and corrective actions, system security activity reviews, information access management, training, education, and awareness, access and acceptable use, physical security, security incidents, and system availability.</p> <p>Security Safeguard Checklist: WISHIN has developed a checklist for Participants to ensure they are adhering to the appropriate security safeguards for onboarding and accessing the HIE.</p> <p>WISHIN Practices: WISHIN will enforce all policies related to security and security incidents. WISHIN will not allow participants to onboard/access the HIE until they have complied with the safeguard checklist. WISHIN has or is developing procedures in conjunction with its policies, to ensure all policies are followed and enforced.</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
Accountability	<p>Policy 700: Workforce, Business Associates, and Contractors – Each Participant shall implement procedures to hold authorized users, business associates 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. Such corrective action measures may include, but not be limited to, retraining, verbal and written warnings, demotion, and/or termination. 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. 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. 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</p>	<p>Privacy Policies are published on WISHIN's website, which is available to the public.</p> <p>Privacy Policies are also made part of the data sharing agreement between participants and WISHIN; participants agree to abide by WISHIN's privacy policies by means of their signature on the data sharing agreement.</p>	n/a

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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.</p> <p>Policy 1000: Privacy Breaches – Investigations and Mitigation – 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</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>(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. 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</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>or organizations involved in the breach.</p> <p>Policy 1100: Authorized User Controls – Each Participant is responsible to:</p> <ol style="list-style-type: none"> 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 and WISHIN'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 		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>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.</p> <p>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.</p> <p>6. Hold their authorized users accountable for compliance with WISHIN and the Participant's policies and, as applicable, the terms of any Business Associate Agreement.</p> <p>WISHIN is responsible to:</p> <p>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.</p> <p>2. Train and supervise its own authorized users on these policies</p>		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>and the standard terms required by its Business Associate Agreement with Participants.</p> <ol style="list-style-type: none"> 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 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. 		

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing <i>(if needed, use additional documents to describe and insert reference here)</i>
	<p>WISHIN Practices:</p> <p>WISHIN will enforce all policies related to privacy and security incidents. WISHIN has or is developing procedures in conjunction with its policies, to ensure all policies are followed and enforced.</p> <p>The HIE system contains detailed audit logs and reports concerning who had accessed individual patient records, and the information they viewed. These reports can be run by WISHIN or participants.</p>		