NETWORK POLICIES

Abstract

Policies are organized according to subject matter, each containing a described purpose, policy, and references to existing documentation.

Version 3.40
Version numbers are incremented as changes are made.
Minor edits increment the version number by hundredths.
Major edits or dozens of minor edits increment the version number by tenths.
Fundamental shifts or full document rewrites increment the version number by whole numbers.
Note: This document is also known as the “MyHealth Policy Privacy and Security Policies and Procedures.”

Last Revision: 2/8/2024

TABLE OF CONTENTS

PREAMBLE

MyHealth Access Network, Inc. is an Oklahoma non-profit corporation designed to provide common administrative and technological infrastructure to enable the realization of its mission, vision and values for its members. These items are specified in this preamble to its policies so all may be aware of the organization's motivations. It is the intent that these principles be influential in the interpretation and application of the Network's policies.

VISION:

The Network's vision is to dramatically improve health outcomes and health care value for the individuals and whole communities which it serves.

MISSION:

The Network's mission is to achieve and sustain the highest quality healthcare at the best value in the nation using health information resources, technology and expertise.

VALUES:

The Network embraces the following defining values to guide its activities:

- We believe in the 5 rights of health information: Right patient, right provider, and right information at the right time in the right setting.
- We believe in the individual right to privacy and security.
- We value a healthy community.
- We believe in honest and open dealings.
- We value creativity and innovation to improve health.
- We seek to augment and add value rather than own and duplicate.
- We value servant leadership.
- We value and act on the input and guidance we receive from the communities we serve.
- We encourage collaboration and the free exchange of ideas with other organizations who share our values.

NETWORK POLICIES

POLICY 1: NETWORK POLICIES, COMPLIANCE, RESPONSIBILITIES AND UPDATES

PURPOSE:

All capitalized terms are defined terms, having the meaning set forth with their first use, or in the Glossary at the end of this document. The Network is authorized, as a Business Associate of its Participants, to store and manage PHI on behalf of its Participant Suppliers for the purposes permitted by Network Agreements (which include these Policies). The Network does not own the data supplied by its Participant Suppliers. The Network is also authorized, as a Business Associate of its Subscribers, to store and manage PHI on behalf of its Subscriber Suppliers for the purposes permitted by its Subscriber Agreements, which must be consistent with those purposes described for Subscriber Suppliers in these policies.

As required by 45 CFR § 164.316, the Network must implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements set forth in the applicable provisions of HIPAA and the HITECH Act. Additionally, the Network is a "health information exchange", and must not engage in "Information Blocking" practices, as these terms are defined in subpart A of the Information Blocking Rule. Accordingly, the Policies are intended to define the consistent and non-discriminatory practices under which the Network will fulfill or not fulfill requests to access, exchange or use EHI, in accordance with the exceptions described in subparts B and C of the Information Blocking Rule. Accordingly, the Policies are designed to enable Participants to leverage MyHealth to address many interoperability requirements under the Information Blocking Rule.

POLICY:

INCORPORATION OF POLICIES INTO AGREEMENTS

The Network will maintain Policies (this document) which will be recognized as the MyHealth Privacy and Security Policies and Procedures, or as the Network Policies, as referenced in the MyHealth Participation Terms and Conditions. These Policies will specify generally how the Network will fulfill its obligations, must be approved by the Board of Directors of the Network, and may be amended from time to time in accordance with the process specified in this Policy #1.

In addition, the Network's Workforce must develop, maintain and amend, as needed, procedures which will correspond to these Policies for the Network's Workforce, Participants and Subscribers to depend on for details about the implementation of the Policies. Said procedures will detail the process for the Network's Workforce, Participants and Subscribers (as applicable) to use in order to implement the Policies which apply to multiple Network Systems. Multiple procedures may be needed to implement certain parts of the Policies depending on the application in different Network Systems.

Policies and procedures will be maintained in written (may be electronic) form. If an action, activity or assessment is required to be documented, the Network must maintain a written record of the action, activity or assessment. The Network must maintain the documentation of Policies and procedures for 10 years from the date when they were in effect. The Network will make the Policies publicly available, and will make other documentation available to those persons responsible for implementing the Policies and/or procedures to which the documentation pertains. The Network must review all documentation periodically and update it as needed, in response to environmental or operational changes affecting the security of the electronic Protected Health Information (PHI).

DATA RESPONSIBILITY AND RECORD RETENTION

The Network will retain the current version of PHI as provided to the Network by Data Suppliers. "Current version" means the most complete record of patient data as provided by the Data Supplier, regardless of the age of that data. The Network may also retain historical PHI.

The Network is not responsible for retaining information used by clinicians for medical decisions. Authorized Users who use PHI from the Network for patient care are responsible for making it part of their own medical records.

If a Participant Supplier leaves the Network, the PHI provided by the Participant Supplier will be returned or destroyed by the Network if required by the Participant Supplier, and if possible, in accordance with the Network Agreement. If a Subscriber Supplier leaves the Network, the PHI provided by the Subscriber Supplier will be handled in accordance with the terms of its Subscriber Agreement.

ASSIGNMENT OF OVERSIGHT RESPONSIBILITIES FOR THE NETWORK

The Network must appoint a Privacy Officer who will be responsible for compliance with and enforcement of the provisions of the HIPAA Privacy Rule. The Network must appoint a Security Officer who will be responsible for compliance with and enforcement of the provisions of the HIPAA Security Rule.

COMPLIANCE WITH THE LAW AND NETWORK POLICIES

These Policies must comply with the Terms and Conditions of the Network Agreement signed by each Participant, to the extent the Terms and Conditions align with Applicable Law. Any conflicts between Policies and the Network Agreement's Terms and Conditions, or differing interpretations, will be interpreted using the language of the most recently adopted document. The resolution of any issues that are not contemplated by the Policies or Network Agreement's Terms and Conditions, or conflicts over interpretation, will be resolved through the Network's governance structure. The final determination in such cases will be decided by the Network's Board of Directors.

The Network and its Participants must comply with all applicable Policies, and all applicable federal, state, and local laws and regulations including, but not limited to, the Information Blocking Rule, and those protecting the confidentiality and security of PHI and the establishing of certain individual privacy rights. These laws and regulations also include privacy principles of use limitation; security safeguards and controls; accountability and oversight; data integrity and quality; remedies; workforce training; sanctions for privacy/security violations, and the reporting of violations.

Participant Suppliers will be responsible for the content of the Data which they supply to the Network, and have the responsibility to include the content that they are required to share in the Information Blocking Rule under the Content and Manner Exception – Content condition at 45 CFR §171.301(a). Network may advise Participant Suppliers of potential compliance issues. Network will have the responsibility to comply with the content and manner requirements in the Information Blocking Rule only to the extent such information has been received by the Network. Network will require Subscriber Suppliers to be responsible for complying with the content and manner requirements in the Information Blocking Rule in connection with Data they supply to the Network.

The Network and Participants will use reasonable efforts to stay abreast of any changes or updates to interpretations of such laws and regulations to ensure compliance. Internal policies and procedures will

be promulgated as required to provide essential privacy protections for patients, and to avoid information blocking.

In the event of a conflict between Network Policies and a Participant's own policies and procedures, the Participant must comply with the policy that is more protective of individual privacy and security, unless that policy would violate the Information Blocking Rule, in which case the Participant must comply with the policy that does not violate the Information Blocking Rule.

Network will require Subscribers to comply with their Subscriber Agreements, which must align with Subscriber obligations in these Policies, and applicable laws.

SANCTIONS AND ENFORCEMENT

The Network and each Participant must maintain and enforce procedures to discipline and hold members of the Workforce accountable for failure to comply with the Network's Policies. The Network must impose sanctions on its Workforce members who are found to be non-compliant with these Policies or any federal, state or local law. Such sanctions may include, but not be limited to, verbal or written warnings, required retraining, suspension without pay, and termination of contract or employment.

Any failure by a Participant's Workforce member to comply with a Participant's HIPAA Privacy and Security Policies will be handled according to the Participant's HIPAA Privacy and Security Policies.

Subscriber Agreements will require Network and Subscribers to comply with applicable law, with respect to maintaining and enforcing procedures to discipline and hold members of their own Workforce accountable for compliance with applicable laws.

The Network's Participants and Subscribers, to the extent provided by law, are responsible for the acts and omissions of their Workforce. The Network will impose sanctions on a Participant or Subscriber whose Authorized Users fail to adhere to these Policies. Such sanctions may include, but not be limited to, verbal and written warnings, suspension of Data Recipient access or Data Supplier data feeds, mandated termination of individual Authorized User access, and termination of participation in the Network.

COMMUNICATION ABOUT POLICIES

The Network will post information regarding privacy and security on its website to help inform the public regarding how key privacy and security issues are managed. Information for the public will be developed and monitored by the Network.

These Policies will also be posted on the Network's public website, for the benefit of Participants, potential Participants, and the general public, and must be kept current. They will be accessible at http://myhealthaccess.net/policies.

REVIEW AND AMENDMENT OF NETWORK POLICIES

These Policies will be reviewed by the Network's Privacy Officer periodically, but at least annually, to determine compliance with applicable laws, regulations, and accreditation standards. Amendments to these Policies may be proposed through the governance processes of the Network. Prior to proposing policy amendments, the Network will consider to what extent Participants will in turn need to amend their Notices of Privacy Practices (documents required by HIPAA informing patients of how their PHI is

being used), and will evaluate other impacts to Network Participants in conjunction with the Network's governance review process. These Policies may be amended by a vote of the Network's Board of Directors. The Network must provide written notice to all Participants of any changes to the Policies at least thirty (30) days prior to the effective date of the change. However, if the change is required in order for the Network and/or Participants to comply with applicable laws or regulations, the Network may implement the change within a shorter period of time if the Network determines it appropriate under the circumstances. The Network must notify Participants immediately in the event of a change required to comply with applicable laws and regulations.

Participants may object to changes in accordance with Policy 2: Participant Objections for Amendments or Inter-HIO Expansion.

The preamble to the Policies are determined by the Board and are not subject to the above process.

REFERENCES:

- 45 CFR § 164.316
- 42 USC § 300jj-52, titled the "21st Century Cures Act"
- 45 CFR § 171.103(a)(2)
- 45 CFR § 171.201-203
- 45 CFR § 171.301(a)
- 24 Okla. Stat. § 161, et seq., titled the "Security Breach Notification Act."
- MyHealth Terms and Conditions 3.2, 10.3(b)(i) & (iii)

Effective Date: 4/1/2024
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Added language relating to the Cures Act and Information Blocking Rule, including the concept of a Subscriber (vs. Participant), differences and similarities of Subscribers, the requirement for Participant Suppliers to include all required data elements, and legal references to Information Blocking Rule. Removed references to expired agreements.
- 2/8/2024: Updated retention period for Policies to 10 years, and made adjusted capitalized terms to clarify references to Policies.

POLICY 2: PARTICIPANT OBJECTIONS FOR AMENDMENTS OR EXPANDED DATA SHARING

PURPOSE:

The governance structure of the Network is designed to invite Participants to be engaged in the decision-making processes of the Network. However in the case that a Participant objects to a vote of the Network's Board of Directors to amend the Policies, or in the case that a Participant objects to the terms for sharing Data or for compliance with applicable laws that are contained in a new agreement made by the Network (which the Network may make in accordance with Policy 9: Use and Disclosure of PHI), a Participant may object within 30 days.

POLICY:

When the Board of Directors votes to amend the Policies, or when the Network authorizes the exchange of PHI under a new contractual arrangement, such as a Subscriber Agreement or an Inter-HIO Agreement, notification of the change must be made to the Authorized Administrators of each Participant.

If a Participant determines that the change affects one of its material rights or obligations under its Agreement, and the Participant objects to the change, the Participant may, within thirty (30) days following the Network's notice of the change to the Participant, (a) make request to the Network for reconsideration, noting the reasons for the Participant's objection; (b) request to have Participant's PHI excluded if their objection relates to an exception under the Information Blocking Rule; or (c) if the objection is based on an amendment to Policies (and not based on a new agreement made by the Network for sharing Data), Participant may terminate its Network Agreement by giving the Network written notice thereof, which may be effective immediately unless a future date is agreed upon with the Network.

When an objection is raised to a particular Policy amendment, the change will be rolled back, or will not—if possible—be implemented with respect to the objecting Participant, until resolution of the reconsideration request or the stated effective date of termination, unless such change is required in order for the Network and/or Participants to comply with applicable laws or regulations.

When an objection is raised to a new contractual arrangement for the Network to exchange PHI, the data sharing arrangement will not—if possible—be implemented with respect to the objecting Participant, until the Participant's objection has been addressed under this Policy.

REQUEST FOR RECONSIDERATION OR EXCLUSION BASED ON A POLICY AMENDMENT

In the event a Participant requests reconsideration or exclusion based on a policy amendment, the Board of Directors must review the request and make a determination thereon within sixty (60) days of its receipt of the request. The determination must be finalized and must be conveyed in writing to the Participant at least five (5) business days prior to becoming final.

REQUEST FOR RECONSIDERATION OR EXCLUSION BASED ON A NEW DATA SHARING ARRANGEMENT

In the event a Participant requests reconsideration or exclusion based on a new data sharing arrangement, the Network must review the request and finalize a determination thereon before proceeding with the data sharing arrangement in a way that would affect Participant, unless required to proceed with the data sharing arrangement under applicable law. If Network is required to proceed with

the data sharing arrangement under applicable law, Network will take any possible steps to limit the impact to Participant, and will advise Participant of the actions being taken and why.

To finalize the determination, the Network will propose its determination in writing to the Participant, the proposed determination will become final in five (5) business days, unless Network agrees in writing to extend the consideration time frame or Network and Participant agree in writing to finalize the determination. After a determination has been finalized, the Network may proceed with the new data sharing arrangement, consistent with the finalized determination.

TERMINATION BASED ON OBJECTION

In the event a Participant chooses not to request reconsideration or exclusion, or is still unsatisfied based on the response or determination to Participant's request, Participant may, within 30 days, terminate its Network Agreement by giving the Network written notice of termination pursuant to this policy and/or the terms of its Network Agreement. Such termination will be effective upon receipt of the notice, unless a future date is agreed upon between the Network and the Participant.

REFERENCES:

- Policy 1: Network Policies, Compliance, Responsibilities and Updates
- Policy 9: Use and Disclosure of Protected Health Information (PHI)
- MyHealth Terms and Conditions 4.7

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 3/12/2018: Updated policy such that new contractual arrangements require explicit authorizations, replacing language before that required explicit authorization for another health information organization.
- 11/2/2020: Adapted objection rights to differentiate and between objections to Policy changes and objections to new data sharing agreements (based on differences in how these are created in Information Blocking Rules). Participant's rights to exclude data must align with Information Blocking Rule exceptions. Participant's termination right to terminate based on objection must be exercised within 30 days.

PATIENT RIGHTS AND PREFERENCES

POLICY 3: PATIENT PREFERENCE

PURPOSE:

The Network values the Individual's right to privacy. The Network also values having the right information about the right patient available to the right provider at the right time in the right setting. This policy discusses how the Network aims to balance these values.

As used in this policy, Individual means the person who is the subject of the PHI, as defined in 45 CFR § 160.103. An Individual's personal representative is one who has authority to act on behalf of the Individual who is the subject of the PHI, according to the criteria defined in 45 CFR § 164.502(g).

POLICY:

COMPLIANCE WITH LEGAL REQUIREMENTS

PHI will be used, accessed, created and disclosed only as permitted under the HIPAA Privacy Rule. With regard to HIPAA, the Network stores and manages Individuals' PHI as a Business Associate of its Data Suppliers under the terms of the Network Agreements (for Participants), and under the terms of Subscriber Agreements (for Subscribers), which will conform with the guidelines for Subscribers as outlined in these Policies. Storage of data on behalf of Participant Suppliers is not a Disclosure (45 CFR § 164.501).

For Sensitive Information—as defined in the Glossary—Data Suppliers are responsible to obtain appropriate authorization from the Individual or the Individual's personal representative prior to submitting such PHI to the Network, and must provide documentation of such authorization to other Network Participants upon request.

NETWORK'S RESPECT FOR PATIENT PRIVACY PREFERENCES

The Network provides a method for any Individual, or an Individual's personal representative (as defined in 45 CFR § 164.502(g)) to opt out of the sharing of their PHI through the Network, as well as a method to revoke the opt-out request.

Minors may make their own opt-out requests in instances in which they may legally consent for their own health services, as outlined in 63 Okla. Stat. §2602 A (1)-(7), 42 CFR Part 2, or other applicable law, as verified by the Participant.

Providers and payers must not condition treatment or coverage on an Individual's willingness to permit access to their PHI through the Network.

INFORMING PATIENTS ABOUT THE NETWORK

The Network must provide information about an Individual's option to opt out or to revoke the opt-out request, along with the necessary forms in the Network office, and on the Network's website in a prominent position. The website, the opt-out form and the opt-out revocation form must describe the effect of opting out in plain language, with complete instructions for submitting the form.

Participants will make available to Individuals information about how their data may be accessed via health information exchange, and the option and process to opt out utilizing Network-provided or Network-approved educational materials in ways that can reasonably be expected to be seen by

Individuals in the due course of their interaction with Participants. Participants are responsible for accurately representing the opt-out opportunity to Individuals, and may provide additional patient education opportunities with their notice of privacy practices, or other methods in cooperation with the Network. Subscribers will be required to provide transparency for patients so they can be informed that their data is being shared through MyHealth, and that they have the opportunity of opting out through MyHealth. This is to be included in information they make available to Individuals about privacy.

Some Data Suppliers, such as behavioral health facilities, may provide additional patient preference policies based on their technical and procedural capabilities. However, compliance with any additional patient preferences beyond those supported by the Network is the responsibility of the individual Data Supplier, and not of the Network.

PROCESS OF OPTING OUT OR REVOKING THE OPT-OUT REQUEST

An Individual or an Individual's personal representative may opt out, or may revoke an opt-out request, at any Participant location or through means accommodated by a Participant or Subscriber, by completing and submitting the appropriate standard form provided by the Network, or a compatible substitute for the form that has been approved by the Network and that correctly communicates the effect of the opt-out choice. The Participant or Subscriber receiving the form or its substitute must verify that the Individual's information is complete, including identity, must sign the form or otherwise authorize its substitute in an approved way by the Network, and immediately forward the form or its substitute to the Network. Alternatively, an Individual or an Individual's personal representative may opt out, or may revoke an opt-out request, by completing and submitting the appropriate standard form, which is provided at the Network's website, or by any Participant or Subscriber, then signing and having the form notarized by a Notary Public, and mailing or delivering to the Network as instructed on the form. An Individual's personal representative who submits a notarized form must also supply evidence of his or her authority to act on behalf of the Individual.

Opt out requests that are properly completed and submitted according to the instructions on the Network's standard form, or according to an approved substitute procedure, must be processed immediately during business hours, upon receipt by the Network. Then, the Network will mail a letter to the Individual's provided address, confirming action on the Individual's request.

If required information is absent or illegible, the form or its substitute has been altered, or the request is unable to be honored for any reason, the Network will communicate, as necessary and appropriately, with the requesting Individual or the Individual's personal representative as well as the submitting Participant or Subscriber, if applicable, and as appropriate, in order to resolve the issue that is preventing the request from being honored.

The Network must retain a copy of each opt-out or opt-out-revocation form received, or records of the substitutes received, with a record of the corresponding actions taken.

EFFECT OF OPTING OUT

To opt out means that an Individual's PHI will be inaccessible to Data Recipients and to parties of authorized HIO-to-HIO data sharing relationships (as described in Policy 9) through the Network Systems, except for the Individual's demographics, and for exceptions outlined below. An Individuals' demographics must remain accessible in order to identify records associated with the Individual to which the opt-out request applies, and to otherwise manage essential activities in the Network System.

When an Individual's opt-out request is revoked, the Individual's PHI, both past and present, regardless of the Individual's opt-out status at the time the PHI was produced, becomes available to Data Recipients through the Network Systems.

An Individual's opt-out request within the Network will be global, meaning that the request to opt out is applied to all Participants, Subscribers, HIO-to-HIO interfaces, other connections, and applications which the Network has the ability to control.

CLARIFICATIONS REGARDING THE SCOPE OF THE EFFECT OF OPTING OUT

An Individual's request to opt out of the Network does not prevent health care professionals from communicating with one another about the care of the Individual.

Application functionality that facilitates Health Care Operations (meaning the activities specified in 45 CFR §164.501 to the extent that the activities are related to covered functions of the Participant), including the use of De-identified Data for quality improvement activities, is not restricted based on an Individual's opt-out request.

EXCEPTIONS TO UNAVAILABILITY OF PHI FOR INDIVIDUALS WHO OPT OUT

EXCEPTION: PUBLIC HEALTH REPORTING

If a Data Supplier is permitted or required to disclose PHI to a government agency for the purpose of public health reporting without an Individual's consent under applicable state and federal laws and regulations, the Network may make that disclosure on behalf of the Data Supplier even if an Individual has requested to opt out.

EXCEPTION: ACCESS OF A MEDICAL EXAMINER OR CORONER FOR A DECEASED INDIVIDUAL

Medical examiners and coroners fulfilling their duties in determining the cause of death are entitled to access medical records under applicable laws independent an Individuals' consent or authorization.

REFERENCES:

- 45 CFR § Part 164
- 45 CFR § 164.312(a)(2)(ii): Emergency Access Procedure
- 42 CFR Part 2
- 42 CFR § 489.24
- 42 CFR § 2.11
- 63 Okla. Stat. §2602 A (1)-(7)
- 63 Okla. Stat. §941
- American Medical Association Policy H-140.989
- MyHealth Terms and Conditions Section 10.3(d)(iii)

Effective Date: 9/11/2023
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Requirement to inform individuals about the Network, including the opt-out option, is now required of all Participants and Subscribers (before it was just Data Recipients), since it is no longer practical under new rules to rely just on the Data Recipient. Consideration for alternative methods to communicate and facilitate the opt-out preference was added.

- 10/12/2021: Exception for coroners and medical examiners added, consistent with legal requirements pertaining to their rights of access in conjunction with updates to Policy 9.
- 8/8/2023: Exceptions for immediate disclosure of records of opted out Individuals have been removed.

POLICY 4: PATIENT HIPAA REQUEST FOR RESTRICTIONS

PURPOSE:

Individuals may request of Covered Entities to restrict the use or disclosure of their PHI, or to maintain confidential communications about their records. Covered Entities may, but are not required to comply with such requests. When considering such requests, Covered Entities who are Data Suppliers to the Network should consider their own, and the Network's ability to comply with an Individual's request.

POLICY:

All Individuals' requests for restrictions or requests for confidential communications must go through the Data Suppliers, not through the Network, except for an Individual's choice to opt out, consistent with Policy 3: Patient Preference.

Participant Suppliers who agree to an Individual's request for restriction on use or disclosure of their PHI, or requests for confidential communications, must comply with such requests with regard to their disclosure of information through the Network. Any items of PHI to which a Participant Supplier agrees to restrict use or disclosure beyond what is permitted through the Network must not be provided to the Network.

The Network will not be responsible for transmitting Individuals' requests for confidential communications among Participants or Subscribers.

If an Individual requests changes in permission or restrictions of Subscriber in relation to how that Subscriber may communicate about that Individual's PHI, Subscriber is responsible for complying with those requests in accordance with their Subscriber Agreement.

If an Individual requests changes in permission or restrictions of a Participant Supplier in relation to how that Participant Supplier may communicate about that Individual's PHI for Permitted Purposes, as described in Policy 9: Use and Disclosure of PHI, Participant Supplier must not agree to comply with such requests without first consulting with the Network to determine whether the Network is physically, administratively, and technologically capable of complying with such changes or restrictions. In case action would be required by the Network to comply with such requests, Participant Supplier must also first obtain the Network's written consent (which will not be unreasonably withheld). Network will not be responsible for any use or disclosure that fails to comply with any such change or revocation that occurs prior to being notified by the Participant Supplier in accordance with this policy.

Individuals seeking to limit the disclosure of their PHI in connection with MyHealth should be advised of their options in accordance with Policy 3: Patient Preference.

REFERENCES:

- 45 CFR § 164.522
- MyHealth Terms and Conditions Section 10.3(d)(iii)

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Added requirements for a Subscriber Agreement to address this HIPAA requirement, and clarified that Data Suppliers have the responsibility not to send data through the network if they agree with the patient to restrictions on data sharing that is allowed by the Network.

POLICY 5: PRIVACY COMPLAINTS AND CONCERNS

PURPOSE:

Any person can make a complaint to a Participant, the Network, or the Secretary regarding the Network's privacy policies and practices, and/or its compliance with its privacy policies and procedures, with a process that complies with 45 CFR §160.306.

POLICY:

The Network, and each Participant must have a process for receiving and tracking complaints regarding privacy or compliance issues from Individuals, Workforce members, or other organizations. The Network and each Participant must have a designated HIPAA Privacy Officer, and must instruct its Workforce members to report any non-compliance with these Policies in accordance with the Participant's applicable policies and procedures. Subscribers shall be required by their respective Subscriber Agreements to agree with the Network on similar requirements as those outlined in this policy for Participants, as required for compliance with applicable laws.

COMPLAINTS OR CONCERNS RELATING TO THE NETWORK RECEIVED BY PARTICIPANTS

Any complaints/concerns about confidentiality relating to the Network must be reported in writing to the affected Participant's HIPAA Privacy Officer for follow-up in accordance with the Participant's applicable policies and procedures. On completion of an investigation by a Participant for issues relating to the Network, a summary of the investigation's findings and any remedial actions taken must be sent to the Network's Privacy Officer.

REGARDING COMPLAINTS OR CONCERNS RELATING TO THE NETWORK RECEIVED BY NETWORK WORKFORCE

Any complaints/concerns about confidentiality relating to the Network received by Network workforce members must be reported to the Network's Privacy Officer for follow-up in accordance with the Network's applicable policies and procedures. Network procedures must require Network personnel to quickly investigate the issue and respond in a timely manner.

In the event the Network identifies issues originating with one or more Participants, Network personnel must act quickly to remediate any issues, possibly involving temporary suspension of Participant access.

If a Participant is found by the Network, pursuant to a complaint or concern received by the Network, to have a problem related to the complaint or concern that requires remediation, the Participant's Authorized Administrator will be notified by the Network, and Participant must provide a report in writing within 30 days of receiving the notification. The written report must describe the event, the cause, action taken to resolve the problem, action taken to prevent recurrence of the problem, and any action taken with involved users, if relevant.

Upon completion of an investigation by the Network for issues relating to any Participant, a summary of the investigation's findings and any remedial actions taken must be sent to the affected Participant's Privacy Officer.

In all cases, the Network's Privacy Officer must archive summaries of the complaints/reports for required reporting and other purposes.

PARTICIPANT SUPPLIERS

Participant Suppliers may request and receive audit logs for a specific patient of the Participant Supplier in response to a complaint and/or a request for accounting of disclosures (see Policy 6: Accounting of Disclosures). Subscriber Suppliers will also be enabled by the Network to meet their requirements for responses to patient requests for an accounting of disclosures, as it pertains to transactions through the Network, based upon the terms of Subscriber Agreements.

ENFORCEMENT

Participants and the Network must enforce the confidentiality provisions of these Policies and the Network Agreement by appropriately disciplining Workforce members who violate the confidentiality of PHI relating to each organization's respective policies. Subscribers must be required to enforce the confidentiality provisions of their Subscriber Agreements and applicable law in accordance with the law on their own Workforce members and subcontractors.

NO DISCRIMINATION

The Network and its Participants must prohibit any member of their respective workforces from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against an Individual for the exercise by that Individual of any right under the Privacy Rule or the Security Rule. No person must be asked to waive his or her rights, including the right to file a complaint with the Secretary, as a condition of treatment or payment. Subscribers must similarly be required to comply with applicable law as it pertains to these principles.

REFERENCES:

- 45 CFR § 160.306, 45 CFR § 164.520(b)(vi); 164.530(a), (b), (d), (g), (h)
- 42 CFR § 482.13(a)(2)(2001) (Medicare Conditions of Participation)

Effective Date: 4/1/2024
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Added requirement to include this HIPAA obligation in agreements with Subscribers.
- 2/8/2024: Capitalized the word "Policies" to clarify its intended use.

POLICY 6: ACCOUNTING OF DISCLOSURES

PURPOSE:

The Network is obligated to support the need of Data Suppliers to honor an Individual's legal right to receive an accounting of disclosures of the Individual's PHI.

POLICY:

Requests for an accounting of disclosures must be made by Individuals to the Data Supplier contributing the Individual's data. The Network must provide information to a Data Supplier in order for the Data Supplier to respond to an Individual's request for an accounting of disclosures of his/her PHI. The Network's response must be made within a time and manner reasonably designated by the Data Supplier in order to permit the Data Supplier to respond to a request by an Individual for an accounting of disclosures. Individuals who contact the Network directly to request an accounting of disclosures for PHI will be given information on contacting Network Data Suppliers with their request, unless the Network is otherwise required under applicable law, in which case the Network will comply with applicable law.

REFERENCES:

- 45 CFR § 164.528
- MyHealth Terms and Conditions Section 10.3(b)(xii)
- Policy 5: Privacy Complaints and Concerns
- Policy 11: Audit Reporting

Effective Date: 4/1/2024
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Adjusted terminology to include Subscribers, and a provision to allow Network to address this topic with directly with patients in any instance that may be required by law.
- 2/8/2024: Revised the purpose to better describe the obligation, and remove the time period from this Policy's purpose (addressed in Policy 11).

POLICY 7: AMENDMENT OF DATA

PURPOSE:

Data Suppliers must comply with applicable federal, state and local laws as well as HIPAA regulations regarding an Individual's right to request amendment and/or correction of PHI, maintained in a designated record set, as defined by 45 CFR § 164.526. The Network must direct all such requests to Data Suppliers.

POLICY:

All requests for amendments must go through the Data Supplier that is the source of the data to be amended or corrected and not through the Network. If any such requests are received by Network, the Network must refer such requests, or the Individuals making such requests, to Data Suppliers, unless the Network becomes required under applicable law to respond differently, in which case the Network will comply with applicable law, in cooperation with the Data Supplier.

If an Individual requests, and the Data Supplier accepts, an amendment, modification or addition to the PHI about the Individual which has previously been provided to the Network, it is the Data Supplier's responsibility to make reasonable attempts to inform Data Recipients that have accessed or received such information through the Network. The Network will provide applicable audit logs to Data Suppliers upon request in accordance with Policy 11: Audit Reporting.

REFERENCES:

- 45 CFR § 164.526
- MyHealth Terms and Conditions Section 10.3(b)(ix)
- Policy 11: Audit Reporting

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Adjusted terminology to include Subscribers, and a provision to allow Network to address this topic directly with patients in any instance that may be required by law. Also clarified Network's commitment to support Data Suppliers with audit records in connection with any need they may have to notify past recipients of information that has changed.

DATA PRIVACY SAFEGUARDS

POLICY 8: MINIMUM NECESSARY ACCESS

PURPOSE:

The Network, Participants and Subscribers must provide essential privacy protections for Individuals by accessing and disclosing only the minimum necessary information in order to accomplish the intended, permitted purposes when PHI needs to be accessed or disclosed, in accordance with the Minimum Necessary Standard defined in HIPAA.

POLICY:

The Network's policy will be to limit the use and disclosure of PHI by all of the Network's Workforce members to the minimum amount of PHI necessary to accomplish their job duties or functions. The Network must make reasonable efforts to limit use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.

The Network's Workforce and Participant's Authorized Users, when working with the Network, must limit the disclosure of PHI, to the extent practicable, to the necessary Limited Data Set, or must use or disclose only the minimum amount of PHI obtained through the Network as necessary to accomplish the intended purpose for which the information was accessed. Accordingly, such necessary disclosures must be limited to only those identified Workforce members, agents and contractors who need the PHI in connection with their job functions or duties.

The Minimum Necessary Standard does not apply to the following:

1. Disclosures to or requests by a health care provider for treatment;
2. Uses or disclosures made to the Individual (if permitted by other policies);
3. Uses or disclosures made pursuant to an authorization;
4. Disclosures made to the Secretary for purposes of enforcing the HIPAA Privacy Rule or Security Rule;
5. Uses or disclosures that are required by law to the extent they are limited to the relevant requirements of such law (but not disclosures that are merely permitted by law); and
6. Uses or disclosures that are required for compliance with any regulation implementing the Administrative Simplification provisions of HIPAA.

For all uses, disclosures, or requests to which the minimum necessary standard applies, the Network must not use, disclose, or request the entire medical record, unless it can specifically justify the entire medical record as the amount necessary to accomplish the purpose of the use, disclosure or request.

Similar terms shall be incorporated in all of the Network's data sharing agreements where PHI is exchanged.

REFERENCES:

- 45 CFR §§ 164.502(b), 164.514(d) & (e)
- MyHealth Terms and Conditions Section 10.3(b)(ii), 10.3(c)(i)

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Added requirement for Network to include this obligation in Subscriber Agreements.

POLICY 9: USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)

PURPOSE:

The Network must use and disclose PHI only as permitted or required by law (as "required by law" is defined in 45 CFR § 164.103), and its legal agreements, and must not engage in any practice that constitutes information blocking (as "information blocking" is defined in 45 CFR § 171.103). PHI used or disclosed by the Network must be for a permitted purpose, and must comply with approved processes.

POLICY:

PERMITTED PURPOSES

As a Business Associate of multiple Covered Entities under HIPAA, the Network may use or disclose PHI for the following purposes, provided that such use or disclosure would not violate state or federal law if performed by the Covered Entities:

- Disclose PHI for treatment, payment, or health care operations purposes, as defined by 45 CFR § 164.501;
- To coroners and medical examiners consistent with 63 O.S. §941 and 45 CFR § 164.512(g)(1);
- To organ procurement organizations, tissue banks and eye banks consistent with 63 O.S. §2200, 45 CFR § 164.512(h) and 42 CFR §482.45;
- To a Data Recipient based on a valid authorization for the unrestricted release of an Individual's medical record, consistent with 63 O.S. §1-505.2 and 45 CFR § 164.508;
- To the Individual in order to fulfill a request to access, exchange or use electronic health information (EHI), as defined by 45 CFR § 171, subject to Policy 22: Requests for Access to Records by an Individual.
- To conduct the Network's operations, including maintenance, reporting, monitoring, troubleshooting, and other essential activities to support its role in its Agreements;
- Subject to the approval process in Policy 10: Analytics and Research, PHI may be used and disclosed for any purpose consistent with HIPAA and other Applicable Law not otherwise permitted by this policy;
- For research, subject to the approval process in Policy 10: Analytics and Research. Research is defined as a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge;
- For public health activities, as described in 45 CFR §164.512(b), and for public health reporting, to the extent the Network is authorized to provide required reports on behalf of Data Suppliers, or the Network approves public health uses under the process described in Policy 10: Analytics and Research.
- For purposes explicitly authorized in writing by the Data Supplier.

Any expansion beyond these functions must be approved by the Board of Directors (MyHealth T&C 1.2(d)), and must be consistent with applicable agreements, laws and regulations.

Data Recipients and Subscriber Recipients may access PHI through the Network only for permitted purposes under these policies and applicable agreements.

Data Suppliers recognize that once PHI has been disclosed to a Data Recipient through the Network for a permitted purpose, that PHI may be incorporated into the Data Recipient's medical record, at which time the privacy and security of that PHI, including control over further downstream uses or disclosures

of such PHI, will become the responsibility of the Data Recipient and is no longer subject to the control of the Data Supplier or the Network.

PROHIBITED PURPOSES

The Network and its Data Recipients must not use the Network System or PHI from Participants for the following prohibited uses, as they are described in the MyHealth Terms and Conditions Section 6.3:

- No Services to Third Parties as described in the MyHealth Terms and Conditions Section 6.3(a).
- No Use for Comparative Studies. Note that specific exceptions to this may be allowed through the process identified in Policy 10: Analytics and Research, with all necessary approvals (MyHealth Terms and Conditions 6.3(b).
- No fundraising or marketing (as defined in 45 CFR § 164.501).

GUIDING PRINCIPLES FOR USE AND DISCLOSURE OF PHI

The Network and its Participants must observe the following:

A. No Data Recipient has rights to the Network Systems except as explicitly granted under the terms of applicable agreements and these policies. All access to PHI through the Network Systems must be consistent with applicable federal, state and local laws. If applicable law requires that certain documentation exists or that other conditions be met prior to accessing PHI for a particular purpose, Data Recipient must ensure that the required documentation has been obtained or the requisite conditions have been met and must be able to provide evidence of such as applicable.

B. All Data Recipients must use appropriate safeguards to prevent unauthorized use or disclosure of PHI, including administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of that PHI.

C. The Network may use PHI to create de-identified information. De-identified information created in accordance with the HIPAA Privacy Rule (45 CFR §164.514(a)) is not subject to the requirements associated with PHI.

D. The Network must not use or disclose PHI in any manner that violates the Network's Business Associate Agreements.

E. The Network, acting under the authority of Business Associate Agreements with its Data Suppliers, may disclose PHI to vendors that assist in carrying out the Network's authorized activities provided:
    1) The Network requires its vendors to protect the confidentiality of PHI in accordance with the Network's Business Associate Agreements with its Participants;
    2) That the vendors make such information available to Participants only in accordance with the Individual's preference, consistent with Policy 3: Patient Preference, and
    3) All vendors with whom the Network must share PHI to carry out a service for the Network must be required to sign a Subcontractor Business Associate Agreement before PHI is disclosed to the vendor.

F. The Network must make its internal practices, books, and records relating to the use and disclosure of PHI available to Data Suppliers, the Secretary, and any other regulators as required, to demonstrate compliance with its legal obligations.

G. In compliance with its Business Associate Agreements, the Network must notify a Participant Supplier if the Network is served with legal process for information stored on the Network Systems, such as a subpoena, court order or request for production of documents, or if the Network receives any request for disclosure of PHI, including disclosures that are otherwise allowed to be made by a Covered Entity under 45 CFR § 164.512. The Network must refer the issuer of subpoenas and discovery requests to the Participant Supplier of the information requested for response. The Network also may refer legal process to its legal counsel for response. Such requests affecting Subscriber Suppliers will be handled in accordance with Subscriber Agreements and applicable law.

DATA SHARING WITH OTHER HIOS AND DATA SHARING NETWORKS

As health information exchange becomes more prevalent, the ability and necessity to exchange data between the Network and other health information organizations (HIOs), data sharing networks, and Subscribers will become more common. Such connections may make the PHI of Data Suppliers accessible to members of other HIOs, members of other data sharing networks, and others who have a right, under applicable law, to request and receive access to PHI through the Network. New relationships for data sharing shall be established consistent with Policy 21: Fulfilling Requests to Access, Exchange, or Use EHI. The Network will only enter into and maintain data sharing agreements with other HIOs, data sharing networks and Subscribers who enter into appropriate agreements with the Network which require them to be subject to all the terms of applicable law in connection with the type of PHI access they wish to have, and to provide.

To prevent PHI from being shared inappropriately, Network will consult with its Data Suppliers through its governance structures outlined in Policies 18-20, and directly, as needed, to identify PHI which should not be shared under one or more of the exceptions under the Information Blocking Rule. MyHealth will implement controls to prevent the sharing of PHI which is identified as PHI that should not be shared.

The Network may choose to participate in the eHealth Exchange , the Trusted Exchange Framework and Common Agreement (TEFCA), and/or link with other networks, provided the agreement facilitating such transactions has been reviewed by the Network's attorney, problematic issues and conflicts are identified, documented and resolved, and the final agreement has been approved by officers of the Network. All agreements for sharing of Data are subject to review and oversight by the Network's Board of Directors, and the Network will not violate applicable law, including the Information Blocking Rule, by entering into or refusing to enter into appropriate agreements. New agreements for sharing Data shall be announced to the Network's Board of Directors, the Operations Management Committee, and to Participants. Participants may request and will receive either the agreements or the applicable parts of agreements pertaining to the agreements that the Network enters into which pertain to sharing Data from or to Participants, and parts that pertain to compliance with applicable laws. Such a decision is subject to a Participant's right to object and terminate for objection as set forth in Policy 2: Participant Objections for Amendments or Expanded Data Sharing.

Data Suppliers recognize that once PHI has been properly disclosed for a permissible purpose, that PHI may be incorporated into the receiving user's medical record, or may otherwise be considered to have been properly disclosed, at which time the privacy and security of that PHI will become the responsibility of the Data Recipient, under the terms of associated agreement(s) and applicable law.

NETWORK DEMONSTRATION CONFIDENTIALITY AGREEMENT

Potential Participants or Subscribers who are considering an arrangement with the Network may request and receive the opportunity to view PHI of an Individual who is currently under their active treatment if they have signed a Network Demonstration Confidentiality Agreement, under the supervision of the Network's Workforce. The Network Demonstration Confidentiality Agreement must require the potential Participant or Subscriber ("Demonstration Participant") to agree to the following terms:

In the course of the demonstration, Demonstration Participant will be limited to viewing PHI of individuals with whom it, or its contracted partners, has or had a relationship and the PHI must pertain to such relationship. The Demonstration Participant must use the PHI only for the purpose of evaluating the Network and its ability to allow Demonstration Participant to engage in exchange of PHI for permitted purposes under the proposed data sharing agreement. The disclosures are also to allow the Network to engage in its proper management and administration, a central purpose of which is to increase the use of health information exchange to improve patient outcomes.

The Network and Demonstration Participant, for good and valuable consideration, agree as follows:

1. Demonstration Participant agrees to refrain from using or disclosing PHI disclosed under this Agreement for purposes other than as set forth above, and agrees to indefinitely maintain the confidentiality of any and all PHI of which Demonstration Participant may become aware of as a result of the purposes set forth above. Except as provided in the foregoing sentence, Demonstration Participant must not use or disclose any PHI disclosed under this Agreement for any other purpose whatsoever unless ordered to do so by a court of competent jurisdiction, or as requested by the Network, even if Demonstration Participant would otherwise have the ability to use or disclose the PHI under HIPAA or other federal, state, or local law. Demonstration Participant must not make any additional disclosure of the PHI (including, but not limited to, disclosures to other workforce members of Demonstration Participant) without the Network's written consent, even if the disclosure is for a purpose otherwise permitted by this Agreement.
2. Demonstration Participant agrees to immediately notify the Network of any instances of which he or she is aware in which the confidentiality of the PHI has been breached. Such reports must be made to the Network's Privacy Officer.
3. In the event that the Demonstration Participant maintains, uses, or discloses PHI in a manner inconsistent with this Agreement, Demonstration Participant will be deemed to be in material breach of this Agreement and will no longer be granted access to PHI, and the Network will be entitled to pursue any remedies available at law or in equity.
4. Demonstration Participant must not remove PHI in any written or electronic form from the demonstration site or from the method or means used for the demonstration.
5. Demonstration Participant hereby agrees to defend and indemnify the Network from any action, suit, claim, or governmental enforcement proceeding (including any reasonable attorneys' fee associated with them) brought by any individual, entity, or governmental body as a result of Demonstration Participant's failure to comply with the terms of this Agreement.

REFERENCES:

- 42 CFR §482.45
- 45 CFR Part 164, § 164.512

- 45 CFR Part 171
- 45 CFR Part 46
- 45 CFR § 160.103
- 63 Okla. Stat. §941
- 63 Okla. Stat. §2200
- "The Oklahoma Security Breach Notification Act", 24 O.S. §§ 161 – 166; 74 O.S. §3113.1
- MyHealth Terms and Conditions Section 1.2, 1.4, 6.2, 6.3, 7.4, 9, 10.3
- Policy 10: Analytics and Research
- Policy 21: Fulfilling Requests to Access, Exchange, or Use EHI
- Policy 22: Requests for Access to Records by an Individual

Effective Date: 4/1/2024
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 7/12/2019: Added healthcare operations as a permitted purpose, as well care coordination with a broader scope than that defined under HIPAA's treatment definition.
- 11/2/2020: Added the requirement of compliance with the Information Blocking Rule. Revised permitted purposes to include payment purposes. Added permitted purpose for disclosing based on an Individual's request, referring to Policy 22. Clarified permitted purposes include purposes authorized by a Data Supplier. Removed references to expired documents. Removed Policy 10's applicability to de-identified information. Updated HIO-to-HIO section to address all data sharing arrangements, with incorporation of Policy 21 and Network's commitment to consult with governance. Added consideration for Subscribers to Network Demonstration Confidentiality Agreement, with language improvements.
- 10/12/2021: Added permitted purposes 1) to include coroners and medical examiners, and 2) for authorization-based access by Data Recipients.
- 2/8/2022: Added permitted purpose of disclosure for organ procurement organizations.
- 2/8/2024: Revised usage of some defined terms (Participant, Data Recipient, Data Supplier, Network) for clarity, and removed an unnecessary reference to the State of Oklahoma from the requirements for the Network Demonstration Confidentiality Agreement.

POLICY 10: ANALYTICS AND RESEARCH

PURPOSE:

In accordance with the Network's stated purpose to reduce the cost and improve the quality and efficiency of health care, the Network aggregates data, including PHI, from Data Suppliers. This policy governs the uses and disclosures of PHI used for any purpose consistent with HIPAA and other Applicable Law not otherwise permitted by the Network's policies, including research, as those are referenced in Policy 9: Use and Disclosure of Protected Health Information (PHI).

POLICY:

The Network must maintain a Board-authorized process for review and approval of proposed data uses and/or disclosures for any purpose consistent with HIPAA and other Applicable Law, including the Information Blocking Rule, not otherwise permitted by the Network's policies, including research, as these purposes are defined in Policy 9: Use and Disclosure of Protected Health Information (PHI). This process will apply to the development and use of reporting and analytics services involving Community Data, meaning data from multiple Participant Suppliers, and will satisfy the requirements of the approvals required to enable each of the uses that will be defined and adopted in the Network's Terms and Conditions. This process will also include provisions to properly review and route requests based on approvals which are required for each request. Data Suppliers may require that their data undergo approval of an Institutional Review Board ("IRB") or similar type of designee prior to their data being included in the result of one or more approved data requests.

The Network may receive requests for datasets. Participant and Subscriber requests for datasets derived from information that is available to them in the Provider Portal which are for Permitted Purposes, as described in Policy 9, must be submitted on a standard request form and may be filled by MyHealth without further approvals from committees or the Board. For all other requests a requestor ("Requestor") must:

- Complete a standard request form provided by the Network.
- Obtain, if applicable, necessary IRB review and approval.
- Counsel with Network's Workforce to gain feedback and assistance in preparing the request for committee consideration.

Requestors are advised that requests submitted to the Network may require several iterations through committees to obtain full approval. After a request has been submitted to the Network, requests must be reviewed by, and must be approved by each of the following, in order:

- Operations Management Committee
- Network's Board of Directors

Depending on the details of the request, additional approvals may be required from one or more of the following:

- One or more Institutional Review Boards
- Affected Data Suppliers
- Affected Individuals
- Other stakeholders

All reports or services must comply with all applicable Business Associate Agreements and permitted uses. Unless otherwise specified, approved report templates may be reused without requiring new approvals if being used by the same entities for the same purposes with the same parameters.

The Network may withdraw authorization for an approved report at any time without prior notice to the report recipients, but shall only do so in compliance with the Information Blocking Rule.

REFERENCES:

- MyHealth Terms and Conditions Sections 1.2, 9
- Policy 9: Use and Disclosure of Protected Health Information (PHI)

Effective Date: 4/1/2024
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 7/12/2019: Revised for consistency with revisions to Policy 9 made on the same date.
- 9/24/2019: Revised paragraph beginning "Participants in the Network may submit requests…" to allow for dataset requests to forego committee process under described circumstances.
- 11/2/2020: De-identified data applicability to this policy removed, aligning with common industry practice. Added Information Blocking Rule reference. Adjusted committee review process based on processes changed by OMC.
- 2/8/2024: Revised language to indicate data requests need not necessarily come from Participants, for consistency with Policy 21.

POLICY 11: AUDIT REPORTING

PURPOSE:

The Network must set forth appropriate practices to effectively log and audit all Authorized User activity within the Network Systems containing PHI. Accurate logging is critical for the Network to support the appropriate use of data, ensure patient confidentiality, maintain secure operations, support investigations of Breaches and respond to requests about PHI access through the Network.

POLICY:

LOGGING

The Network must log all Authorized User activity including User ID, data source, provider, details about information, time of access, and other relevant Authorized User information to the extent possible (device address, actions taken, justification, etc.). All logged activity must be retained and must be available to the Network's administrative users for ten (10) years. All audit records must be protected against unauthorized access, modifications and deletions.

REQUESTS FOR AUDIT REPORTS

The Network will provide audit log access to Authorized Administrators and appropriate Subscriber personnel based on Subscriber Agreements, in support of their Workforce oversight duties. Participants may request audit logs for activity by their Authorized Users or in connection with investigations. Subscribers may request audit logs for activity in connection with the terms of their Subscriber Agreements. The Network Workforce will maintain a procedure for tracking and responding to audit requests.

MONITORING

User activity pattern observation, system usage habits, automated alerts and other systematic or ad hoc user monitoring may be conducted by the Network's Workforce and by Data Recipients' Authorized Administrators (for their respective Authorized Users). Suspicious activity may trigger additional investigations into possible misuse of the Network Systems.

REFERENCES:

- 45 CFR § 164.312(b), 45 CFR § 164.528
- MyHealth Terms and Conditions Section 12.5
- Policy 6: Accounting of Disclosures

Effective Date: 4/1/2024
Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval
- 11/2/2020: Added consideration for the needs of Subscribers for audit support.
- 2/8/2024: Audit log retention period changed from 6 years to 10 years in compliance with requirements from the State of Oklahoma.

POLICY 12: USER ACCESS TO SYSTEMS CONTAINING PHI

PURPOSE:

The Network, Participants, and Subscribers (as required through their Subscriber Agreements) must ensure that all Authorized User accounts providing access to PHI through the Network Systems are authorized, correctly provided/modified, and removed in a timely fashion. Access to PHI through Network Systems requires authorization in order to ensure the Confidentiality, Integrity, and Availability of the information.

POLICY:

AUTHORIZED ADMINISTRATORS

Subscribers will have comparable requirements in their Subscriber Agreements to those requirements placed on Participants in this Policy.

Each Participant must assign one or more persons in writing as Authorized Administrators (also known as Participant Authoritative Sources, Trusted Security Administrators, or Trusted Sources) who will oversee the day-to-day security surrounding the Network, and must be responsible for establishing and maintaining appropriate access for Authorized Users on behalf of the Participant. Participant must notify the Network of any change in the status of an Authorized Administrator.

Each Participant attests that its Authorized Administrator will be responsible for the following duties:

1) Update account access in the Network Systems, or notify Network Workforce to make appropriate updates, as personnel changes or circumstances warrant changes to Authorized User access;
2) Supply and verify registration information for new Authorized Users, in accordance with Network onboarding procedures;
3) Verify periodically, but no less often than quarterly, the accuracy of the Participant's Authorized Users and their roles;
4) Act as the Network's primary contact for technical problems;
5) Ensure Authorized Users have received training regarding the confidentiality of PHI under state laws, federal laws, and Network Agreements, including the guidelines in this policy;
6) Perform usage audits on Authorized User activity with support of the Network to verify compliance with Participant Recipient and Network privacy policies;
7) Ensure Authorized Users understand that failure to comply with Participant and Network privacy policies carries consequences, which may include the Participant's exclusion from the Network;
8) Understand criteria and ensure only appropriate Workforce members become Authorized Users, assigned to proper roles; and
9) Ensure availability of the Participant's educational materials about the Network and the patient's option to opt out (see Policy 3: Patient Preference).

Each Participant Recipient is responsible to oversee the activities of its Authorized Users, and must be solely responsible, as allowed by applicable law, for all acts and omissions of the Participant Recipient's Authorized Users, and all Individuals who access the Network either through the Participant Recipient or by use of any login credential received or obtained, directly or indirectly, lawfully or unlawfully, from the Participant Recipient or any of the Participant Recipient's Authorized Users.

NETWORK OVERSIGHT

The Network will maintain an active list of Authorized Administrators. The Network will provide a list of Active Users to Authorized Administrators on at least a quarterly basis for review. Authorized User activity reports will also be provided by the Network upon request. The Network may terminate Authorized User and/or Authorized Administrator access to Network Systems immediately or as promptly as reasonably practicable but in any event within one business day of:

- Termination of a Participant's Agreement with the Network;
- Written notification of termination of an Authorized User's employment or affiliation with the Participant; or
- As specified in the Network's Policies (see Sanctions and Enforcement section in Policy 1: Network Policies, Compliance, Responsibilities and Updates) to maintain the security and integrity of the Network.

NETWORK TRAINING AND HELP DESK

The Network will provide training materials which are determined by the Network to be appropriate for Authorized Users to utilize Network's services. Network will provide training support for Participants who wish to provide their own training for Authorized Users.

Network will provide support and assistance to Participants in resolving difficulties in accessing and using the Network services during regular business hours by telephone, email, and/or by other means. Network will have after hours, on-call staff available to assist with emergencies. Contact information for these help desk support services will be provided to Participants by Network.

AUTHORIZED USERS

Only Authorized Users will be able to access Network Systems containing PHI. Authorization for Authorized Users for any Network System must be granted by a Participant Recipient's Authorized Administrator, or by a Subscriber under comparable terms in the Subscriber Agreement, prior to the access being granted. Access authorization records must be maintained for a minimum of ten (10) years.

The Authorized Administrator will specify (or will verify, if the Network is asked to create the logon IDs), for each Authorized User, a unique logon ID and appropriate access roles. Network access to PHI is restricted by the roles and responsibilities for each Authorized User, and the data set for which they have responsibility, in accordance with Policy 8: Minimum Necessary Access.

Each Participant Recipient attests that each Authorized User has been trained on HIPAA privacy and security rules, and any unique aspects for use of the Network at their location. Participant Recipient attests that Authorized Users have also been instructed and have agreed as follows (note: the Network will link to these terms from the User login screen, so the User agrees to these terms by signing on):

- The Authorized User must safeguard his/her distinct logon ID and password, and not allow others to use it.
- The Authorized User must access information only for Individuals within the scope of his/her job responsibilities, only as necessary to perform his/her job responsibilities, and only for purposes approved by the authorizing organization.
- The Authorized User must not disclose any information from the Network to any third party except for permitted purposes.
- The Authorized User must undertake a reasonable and professional degree of care to protect the confidential nature of any information accessed from the Network, and this obligation must

continue during and after termination of any legal relationship with the Network and/or its Participants.

- The Authorized User has received training on HIPAA guidelines and has access to the Network's Privacy and Security Policies (https://myhealthaccess.net/policies), and by accessing the Network Systems, agrees to abide by them.
- The Authorized User must notify his/her authorizing organization, or the Network, as appropriate, immediately of any violation of HIPAA or Network's Privacy and Security Policies of which he/she becomes aware.
- The Authorized User must comply with all applicable federal, state and local laws, rules and regulations with regard to access, use and disclosure of PHI.
- The Authorized User acknowledges that any violation of this Agreement may result in modification, suspension or revocation of his/her access to the Network Systems, and/or disciplinary measures by his/her authorizing organization, up to and including termination of access or employment.
- The Authorized User acknowledges that the Network, Participants and Subscribers have reserved rights to monitor, access and disclose usage information via the Network System, and, therefore, Authorized Users do not have a reasonable expectation of privacy with respect to their use of the Network.

REFERENCES:

- 45 CFR § 164.308(a)(4)
- 45 CFR § 164.530
- Oklahoma H.B. 2245, titled "The Security Breach Notification Act"
- MyHealth Terms and Conditions Section 5, 12.3 and 12.4

Effective Date: 4/1/2024
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 4/8/2019: Removed password expiration, changed administrator review obligations from annually to quarterly, and clarified Network's commitment to facilitate such review.
- 11/2/2020: Added concept of Subscribers with comparable requirements. Added training and helpdesk for completeness, and alignment with current practice (based on T&C Section 12).
- 2/8/2024: Changed retention period for user authorization records from 6 years to 10 years, in compliance with requirements from the State of Oklahoma. Also made minor adjustment to clarify that the declared audit rights apply to all Network members.

DATA SECURITY SAFEGUARDS

POLICY 13: NETWORK PROTECTION OF DATA CONFIDENTIALITY

PURPOSE:

The Network is responsible to properly receive and protect PHI from unauthorized access. The Network must maintain a current risk analysis (45 CFR § 164.308), and must document and implement appropriate procedures to reduce risks of security incidents to reasonable levels (45 CFR § 164.306).

POLICY:

The Network must maintain and comply with a comprehensive information security program ("Security Program") that conforms to the requirements of a properly-scoped HITRUST Common Security Framework r2 Assessment®, authorized by the Network's Security Officer, and either the Chief Operating Officer or the Chief Executive Officer. The Network will further ensure its Security Program incorporates system security requirements which are required for the State Designated Entity for Health Information Exchange by the Oklahoma Health Care Authority, including all necessary physical, administrative, and technical safeguards to maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure or modification of information with the highest reasonable security standards, consistent with HIPAA requirements (45 CFR §164.306-308).

The Network will obtain and maintain certified status with a properly scoped HITRUST CSF r2 assessment. A properly scoped HITRUST CSF r2 assessment incorporates new industry requirements as they evolve, and incorporates applicable controls from NIST SP 800-53, NIST CSF, ISO 27001, HIPAA Security Rule, FedRAMP, FISMA, FTC Red Flags Rule Compliance, MARS-E Requirements, PCI DSS, CCPA, GDPR, AICPA Trust Services Criteria for Security, Confidentiality and Availability, and more than 30 other industry-recognized frameworks, standards and authorized sources (source: https://hitrustalliance.net/content/uploads/r2-Assessments-Datasheet.pdf, accessed 1/22/2024).

If a Data Supplier requests additional safeguards, audits or evidence that are not required under this Policy, Network may, based on the Data Supplier's ownership of that Data, and Network's role as Trusted Holder of that Data, agree to those additional safeguards, at the sole discretion of the Network's Security Officer. Such agreements may be incorporated in a Data Supplier's individual Agreement. In general, if such requirements create additional cost or resource burden to the Network, the requesting Data Supplier should expect the arrangement to include appropriate compensation, out of consideration for others who financially support the Network without special accommodation.

VENDOR CONTRACTS

The Network's applications are hosted by one or more third-party vendors and subcontractors. Vendors are responsible for the physical security of the application and its data by contractual agreement. The Network's contracts with vendors housing PHI must incorporate requirements to comply with all of the obligations of the Network.

NETWORK SECURITY OVERSIGHT

As requested, the Network will provide information security information to the Network's Privacy and Security Subcommittee, and will provide documentation of the status of its security certification, and documentation of its Security Program (with appropriate confidentiality assurances) to requesting Participants and Subscribers, or other appropriate parties.

REFERENCES:

- HITRUST CSF Framework® - (hitrustalliance.net/product-tool/hitrust-csf/)
- Applicable contract(s) between MyHealth and the Oklahoma Health Care Authority pertaining to State Designated Entity designation
- HIPAA Security Rule (45 CFR Parts 160, 162 and 164) – and specifically, 45 CFR § 164.312(e)
- MyHealth Terms and Conditions Sections 7.3, 10.3(b)(i) & (iii)

Effective Date: 4/1/2024
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 4/8/2019: Removed password reset requirement.
- 11/2/2020: Clarified security risk analysis frequency means annually and when changes are made. Added consideration for Subscribers. Added the Network's standard practice pertaining to unique safeguards required by only one stakeholder. Clarified policy of email and PHI in light of widespread TLS encryption. Clarified policy of PHI and international workers. Added three safeguards that are in technology contracts (so Network participants see they exist)—specifically prohibition of identifying markers on data center equipment, Network's handling of physical PHI, and controls for physical systems that host PHI. Updated minimum password length to 12 characters. Removed protocol to email administrators when users' passwords are reset based on lack of effectiveness and practicality.
- 2/8/2024: Replaced specific security requirements with requirement for an "Information Security Management Plan" that conforms with HITRUST and State requirements. Also added requirement for Network to obtain and maintain HITRUST CSF r2 certification.

POLICY 14: NETWORK PROTECTION OF DATA INTEGRITY

PURPOSE:

Each Data Supplier must use reasonable efforts to ensure that PHI it provides to the Network is accurate, free from error, complete (in compliance with applicable law, including the Content and Manner provision of the Information Blocking Rule, at 45 CFR §171.301(a)), and provided in a timely manner. The Network must implement safeguards to ensure that PHI has not been changed/corrupted and to validate that data came from the original sender. However, all of the complexities of health information exchange require that Authorized Users recognize that data presented may not always be accurate. Authorized Users are responsible to verify the accuracy of information they may rely upon. Subscribers will have comparable terms to those in this Policy incorporated in Subscriber Agreements.

POLICY:

DATA SUPPLIER'S ROLE IN QUALITY

Data Suppliers who are Data Recipients are strongly encouraged to audit the display of their data to ensure accurate display of information. Data Suppliers who are not Data Recipients may be authorized to view at least a subset of the data they have submitted to verify its accuracy.

NETWORK INTEGRITY CONTROLS

The Network must implement industry-standard controls to validate that PHI has not been changed/corrupted and to validate that data came from the original sender. The Network will stay abreast of developments in the field of cryptographic message authentication and other fields related to verifying data integrity and authenticity.

The Network may temporarily suspend Network data feeds or access to specific data to protect the integrity of the Network's data.

The Network will utilize advanced matching technology and techniques to identify and link the same Individual's PHI together within Network Systems, and will work with Participants to continually improve the quality of matching over time.

The Network shall maintain association between PHI and the source of that PHI, such that PHI may always be associated with its originating source.

DATA RECIPIENT'S ROLE IN QUALITY

The Authorized User is responsible to verify the accuracy of any information he or she may rely upon from the Network system. Authorized Users must report data accuracy issues to the Network.

REFERENCES:

- 45 CFR § 164.312(c)
- 45 CFR § 171.301(a)
- Policy 1: Network Policies, Compliance, Responsibilities and Updates
- MyHealth Terms and Conditions Sections 7.3, 10.3(b)(i) & (iii), 15.6, 15.7

Effective Date: 11/2/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Incorporated Information Blocking Rule reference and consideration for Subscribers. Inserted specific assurance that PHI is always affiliated with its source. This has always been practiced by necessity to facilitate data ownership provisions but is now stated directly.

POLICY 15: NETWORK PROTECTION OF DATA AVAILABILITY

PURPOSE:

The Network will endeavor to ensure that information systems containing PHI and related daily processing can be recovered following an unplanned event, and will endeavor to ensure that Authorized Users are always able to access the Network Systems for permitted purposes.

POLICY:

DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

The Network will develop and execute a plan to maintain operations in case of unforeseen events, consistent with the Security Program defined in Policy 13, which must satisfy the requirements of the HITRUST CSF r2 certification.

SERVICE LEVEL ASSURANCE

The Network will strive to maintain a level of performance that fulfills the needs of Participants and Subscribers. As a condition of providing services, the Network will establish a standard levels of Service-Level Assurance (SLA) for Participants, which may also apply to some Subscribers depending on the Subscriber Agreements. The Network will track its performance against these Service Level Assurance standards and will report on its monthly performance to the Operations Management Committee. The Network will strive to minimize unplanned disruptions to service. Due to the nature of the sustainability model of the Network, if Participants or Subscribers wish to have financial remedies incorporated into their agreements in connection with the Network's Service Level Assurance performance, the Network may increase their cost of subscription in keeping with guidance from the Network's governance to offset increased financial risk to the organization and enhancement of service level assurance technologies.

In order to perform necessary maintenance and/or to implement improvements to the Network's health IT performance, the Network may be temporarily unavailable, or temporarily degraded in performance during maintenance periods. Maintenance periods may occur on a fixed schedule and may also be scheduled specifically in advance, and shall be published with published Service Level Assurance information, which shall be shared with Participants and some Subscribers.

Any intentional periods of unavailability or degraded performance will be kept as brief as possible, limited to the time necessary to complete the maintenance or improvements. Any planned unavailability or degradation that is initiated by the Network will be consistent with published SLA standards or agreements. Any unplanned unavailability or degradation that is initiated by the Network will be consistent with published SLA standards or agreements.

The Network will notify Users, Participants, and/or Subscribers who are most likely to be affected by planned service outages. When possible, Network will endeavor to notify Users, Participants, and/or Subscribers if extended unplanned service occur, as well.

UNAVAILABILITY TO PREVENT HARM OR IN RESPONSE TO A SECURITY RISK

The Network may be made unavailable for maintenance or improvements that are initiated by the Network in response to either 1) a risk of harm to a patient or another person, or 2) a security risk to EHI. Such unavailability will be limited in scope to address the specific risk for which the Network was made unavailable.

REFERENCES:

- 45 CFR § 164.308(a)(7)
- Policy 13: Network Protection of Data Confidentiality
- MyHealth Terms and Conditions Sections 10.3(b)(i) & (iii)

Effective Date: 4/1/2024
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Modified language based on cloud-computing paradigm (vs traditional data center paradigm). Added service level assurance section and service unavailability provisions based on Information Blocking Rule exceptions.
- 2/8/2024: Disaster recovery plan requirements amended to refer to the Security Program set forth in Policy 13.

SECURITY INCIDENTS AND RESPONSE

POLICY 16: BREACH RESPONSE

PURPOSE:

Subscribers will have terms similar to those in this section under their Subscriber Agreements.

Under HIPAA, the Breach Notification for Unsecured Protected Health Information Rule requires Covered Entities, such as Participants, to notify Individuals and HHS when a Breach of one or more Individuals' PHI has occurred. The Network, as a Business Associate of each Participant, must notify each Participant in a timely manner in the event of a Breach of PHI supplied by that Participant to allow the Participant to notify affected Individuals and HHS. The Network may contact Individuals if requested in writing by the affected Data Supplier(s).

When multiple Participants take part in health information exchange and there is a Breach of unsecured PHI at the Network, the obligation to notify Individuals of the Breach falls to the Participants (as the Participants are HIPAA covered entities). Because of the nature of health information exchange, it may be decided by the Network to notify all potentially affected Participants, and those Participants may prefer to delegate to the Network the responsibility of sending the required notifications to the affected Individuals in order to avoid the confusion of Individuals receiving more than one notification of the same Breach.

Network's contracts with vendors involving PHI must identify the vendor's role in reacting to and being responsible for data Breaches in such a way to enable the Network to comply with its obligations.

POLICY:

BREACHES DISCOVERED BY NETWORK PARTICIPANTS

Network Participants who discover potential Breaches that may involve the use of PHI from the Network should alert the Network within 48 hours. Upon confirmation that a Breach has occurred, then within 24 hours of that determination, the Network Participant must file a written initial report to the Network containing the following:

- One or two sentence description of the Breach
- Description of the roles of the people involved in the Breach
- The type of PHI that was Breached
- Network Participants likely impacted by the Breach
- Number of Individuals or records impacted/estimated to be impacted by the Breach
- Actions taken by the Participant to mitigate the Breach
- Current status of the Breach (under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar Breach

Participant must also make available to the Network reports that are sent to the federal government regarding the Breach according to applicable requirements.

BREACHES DISCOVERED BY NETWORK WORKFORCE

Network Workforce who discover, believe, or suspect that Unsecured PHI has been accessed, used, or disclosed in a way that may violate the HIPAA Privacy or Security Rules, or any non-permitted use of PHI must immediately report such information to the Network's Security Officer, or designee. The Network Security Officer/designee must make an immediate notification of a Breach, suspected Breach, or non-permitted use to affected Data Supplier(s).

Because of the nature of health information exchange, investigation may take some time. However, subsequent to the initial notification, the Network must send a written report to the affected Data Supplier(s) within ten (10) business days or as promptly thereafter as the information becomes available, to include the following, and any additional elements as required by Applicable Law:

- Identification of each Individual whose Unsecured PHI is reasonably believed to have been accessed, acquired, used or disclosed;
- A description of what happened, including the date of the Breach and the date of the discovery of the Breach;
- A description of the types of unsecured PHI that were involved in the Breach;
- Suggested steps affected Individuals should take to protect themselves from potential harm resulting from the Breach;
- A brief description of what the Network is doing to investigate the Breach, mitigate potential harm, and to protect against future Breaches.

The Network must only contact Individuals suspected to be affected by the Breach with prior written request of the affected Data Supplier(s).

In addition to providing notification, the Network will:

1) Investigate the scope and magnitude of the Breach.
2) Identify the root cause of the Breach.
3) Mitigate, to the extent possible, damages caused by the Breach (which may include suspension of Data Recipient access).
4) If applicable, request the party who received such PHI to return and/or destroy the impermissibly disclosed PHI.
5) Apply sanctions as appropriate.

If applicable, Network will report Security Breaches to affected Data Supplier(s) as required by 74 O.S. § 3113.1, titled the "Security Breach Notification Act", as defined therein.

Network must notify the Board of Directors, the Operations Management Committee, and other designees of the Network, of the Breach.

Required notifications and additional Breach response activities will be made in cooperation with affected Participants, the Network, and the Network's Cyber-Liability insurance carrier, as appropriate and required.

REFERENCES:

- 74 O.S. § 3113.1, titled the "Security Breach Notification Act"
- 45 CFR § 164.400-414; 164.530(b), (d), (e), (g), (h), (i), (j).
- "The Oklahoma Security Breach Notification Act", 24 O.S. §§ 161 – 166; 74 O.S. §3113.1
- MyHealth Terms and Conditions Section 10.3(b)(v)

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Incorporated similar provisions for Subscribers. Added a reference to law for elements required in a notification of Breach.

POLICY 17: PRIVACY INCIDENTS OR SECURITY INCIDENTS

PURPOSE:

Subscribers will have terms similar to those in this section under their Subscriber Agreements.

The Network, and each Participant, must have a process by which any person can report Privacy Incidents (improper uses or disclosures of PHI) to the organization's Privacy Officer, and a process for reporting Security Incidents (as defined by HIPAA) to the organization's Security Officer (or comparable role). The Network's procedures must provide for safeguards to help prevent, detect, contain, and correct various security breaches/incidents.

POLICY:

Participants must report any potential or confirmed improper use or disclosure of information from the Network to the Network immediately upon discovery. This immediate reporting requirement is limited to the misuse of data, and threats to the Network's security.

Network Workforce must report any suspected or known Security Incidents to the Network's Security Officer. The Network's Security Officer must respond in accordance with the Network's Incident Response procedure.

The Network's Security Officer must investigate and respond to reported incidents as appropriate, and as directed by Network management in an effort to mitigate any harmful effects of the incident. The Security Officer must maintain documentation of all security incidents and outcomes for a period of ten (10) years or based on applicable regulatory requirements (whichever is greater). Security Incidents will be prioritized and reported to Participants.

Incidents that constitute a Breach or potential Breach will be handled in accordance with Policy 16: Breach Response. Privacy complaints or concerns reported to Network will be investigated and handled in accordance with Policy 5: Privacy Complaints and Concerns.

ENFORCEMENT

Participants and the Network must enforce the provisions of these Policies and the Network Agreement by appropriately disciplining Workforce members who violate them.

REFERENCES:

- 45 CFR § 164.308 (a)(6)
- MyHealth Terms and Conditions Section 10.3(b)(iv)
- Policy 5: Privacy Complaints and Concerns
- Policy 16: Breach Response

Effective Date: 4/1/2024
Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Added consideration for Subscribers.
- 2/8/2024: Updated retention period from 6 years to 10 years for incident response.

NETWORK MEMBERSHIP AND GOVERNANCE

POLICY 18: ORGANIZATION VISION AND GOVERNANCE

PURPOSE:

This policy will describe the parameters under which Network's governance will operate.

POLICY:

The Network's bylaws and approved committee charters will define the manner in which governance in the Network will operate, under the direction and approval of the Board of Directors.

The Board of Directors takes input from the Operations Management Committee (OMC), which fulfills the role of the Participant Council as that term is used in the MyHealth Terms and Conditions Section, as well as the Research Subcommittee. The Privacy and Security Subcommittee also operates under the oversight of this committee. A list of the OMC responsibilities are included in the Charter for the committee, which is available from MyHealth upon request. Every Participant and Subnetwork (as defined in Policy 19: Subnetworks and Interest Groups) is entitled to a vote on the Operations Management Committee, and may send as many representatives as they wish to participate in discussions.

The Board of Directors also takes input from the Clinical Quality Committee, which attracts executive-level leaders from the clinical and quality oversight arenas. This committee provides strategic insight and guidance to the Board. Every Participant is entitled to one vote on the Clinical Quality Committee, and may send as many representatives as they wish to participate in discussions.

Other committees and subcommittees are formed to facilitate discussion and review of pertinent issues, and Participants may learn about these through involvement in the established committees and by discussing with their MyHealth representatives. Subnetworks and Interest Groups, may also meet to discuss pertinent issues to their members' interests.

REFERENCES:

- MyHealth Terms and Conditions Sections 9, 12.6

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Updated policy language to be consistent with how governance committees have chosen to evolve.

POLICY 19: SUBNETWORKS AND INTEREST GROUPS

PURPOSE:

Experience has shown there to be value in groups organizing around common applications or disciplines with regard to health information exchange. Such groups can provide tremendous value for their own constituents, for others they interact with, and for the Network at large by defining best practices for existing uses of data; developing approaches or procedures for handling common situations; devising and developing additional value-added data-driven proposals; encouraging increased membership, and promoting the sustainability of the Network.

To this end, the Network wishes to encourage the formation of such groups. This policy will define the roles these groups will play in governance, and clarify the domains of their intended roles within the Network structure.

POLICY:

The Network will maintain communication and governance procedures that encourage and promote the formation of Subnetworks and Interest Groups, as defined below. To maintain order and promote cooperation within the healthcare industry, the Network will maintain a list of Subnetworks and Interest Groups that have been formally recognized by the Board of Directors. These entities will be defined as follows:

SUBNETWORKS

A Subnetwork is an entity approved by the Network's Board of Directors to receive the Subnetwork designation within the Network. In general, the entity will be a multi-organizational entity, all of whose members are or desire to be Participants in the Network, which is formally organized, and whose stated purpose (as reflected in its organizational structure) is to represent the health information exchange interests of a particular discipline, or a geographical region of significant size. Subnetworks may be organized independently, or may be organized within, or sponsored by, existing entities (such as a professional association) that are modeled on similar principles. However, it is not the intention of the Network that Subnetworks will be permitted which would only represent a subset of a particular profession, or a subset of a particular region, depending upon which division is chosen.

Subnetworks will provide a focused forum for consideration, discussion and resolution of health information exchange issues specific to the needs and interests of its constituents. Subnetworks should be inviting to all Participants of the Network who satisfy the scope of their defined profession or geographical region, and be organized in such a way as to encourage engagement and input from all such parties. Subnetwork members may depend on the Subnetworks to learn about happenings in the Network relevant to them, to contribute ideas, and to raise concerns. The Network may depend on the Subnetworks to consider, discuss and propose resolutions for issues specific to the Subnetwork's profession or region. Subnetworks may request and/or benefit from the expertise of Network committees and subcommittees for assistance with subject-specific issues, such as Privacy and Security, Communications, Clinical/Quality, etc.

Subnetworks will be entitled to cast votes on the Network's Operations Management Committee and the Clinical Quality Committee, and have their representatives' votes explicitly reported to the Board, on the following conditions:

1) The Subnetwork holds regular meetings facilitating participation of their members where health information exchange issues are discussed.
2) These meetings have formal agendas and minutes that are shared with the Network upon request.
3) Network Workforce or governance representatives are welcome to attend these meetings, and meeting participation information is shared with the Network's administrative assistant with the same prior notice given to the Subnetwork's own members.
4) The Subnetwork formally names and authorizes representatives to consistently attend and cast votes for its interests at the Operations Management Committee, and optionally, the Clinical/Quality Committee (proxies may be arranged in advance but attendance requirements of committees must be observed).
5) Those casting votes on behalf of Subnetworks are Participants of the Network and do not derive compensation for representing the Subnetwork.

The Network will support Subnetworks by formalizing communication channels with Network Workforce and leadership of the committees on which they participate, so that to the degree possible, Subnetworks will receive status updates from Network Workforce regarding relevant issues and known upcoming agenda items for the Network's committees and Board of Directors.

Subnetworks may, but are not required, to enter into custom agreements with the Network. Subnetworks may negotiate special pricing and resell the services of the Network in a way that may contribute to their own sustainability as well as that of the Network (note that other entities may enter into agreements to do this also, who may be network resellers and not Subnetworks).

Subnetwork members who utilize Network services must sign an Agreement directly with the Network, which may be a unique Subnetwork version of the standard Network Agreement. Subnetworks may work with the Network to provide additional value to its membership, may apply for and administer grants using data from the Network and may decide to adopt its own branding, procedures, marketing, education and other functions that may be helpful to that Subnetwork, all in keeping with the Network's Agreements and policies. Subnetworks will transparently communicate with the Network about unique versions of Network materials and its activities as they concern the Network as these initiatives develop. If risk or policy issues arise that may affect other Network members, the Network may provide assistance to the Subnetwork in adapting those issues to mitigate risks and ensure policy compliance.

Subnetworks may take time to develop, and organizations that meet significant subsets of the requirements may receive some of the benefits of Subnetworks as permitted by the Board depending on circumstances.

INTEREST GROUPS

An Interest Group is an organized group of interested stakeholders who wish to provide input, organize related initiatives, or otherwise participate in initiatives related to the Network. The Board of Directors will determine which Interest Groups are formally recognized by the Network. Interest Groups may or may not include Network Participants and may represent groups of stakeholders who do not directly participate in the Network (for example: employers). Interest Groups may or may not be legal entities. Interest Groups will be incorporated into formal communication channels to receive timely updates about the status of the Network and issues that may affect their interests, and will have a formal channel through which their input and concerns can be expressed to Network committees and the

Board. Interest Groups do not have voting rights but do have the ability to recommend agenda items and to be recognized as an authoritative voice on the subject matters for which they have been recognized by the Board to hold within their scope of interest.

Generally, Interest Groups that are recognized by the Board will have the following characteristics:

1) The Interest Group will hold regular meetings facilitating participation of their members where health information exchange issues are discussed.
2) These meetings have formal agendas and minutes that are shared with the Network upon request.
3) Network Workforce or governance representatives are invited to attend these meetings. Meeting participation information will be provided to the Network's administrative assistant with the same prior notice given to the Interest Group's own members.
4) The Interest Group has clearly defined its scope of interest, in writing, with respect to the Network in a formal request to the Board for recognition.
5) The Interest Group's members have clear expertise in the subject matters which they have an interest in, and their goals demonstrate reasonable alignment with the objectives of the Network.

Interest Groups may include organizations focused on specific health issues, certain healthcare workflows, regional health committees, subject matter study groups, or similar types of organizations.

REFERENCES:

- MyHealth Terms and Conditions Section 12.6

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 3/30/2016: Updated definition of a Subnetwork—removed legal entity from the definition.
- 11/2/2020: Removed references to governance practices that have changed over time based on Participant preference.

POLICY 20: ELIGIBILITY AND ACCEPTANCE OF NEW NETWORK PARTICIPANTS

PURPOSE:

In order to assure privacy and security of PHI, the Network oversees the approach to Participant eligibility, acceptance, and enrollment. Organizations registered and approved by the Board as Participants, who have signed an appropriate Business Associate Agreement which binds them to these policies will be permitted to access the Network Systems. Entities who are not Participants who request access to EHI consistent with the Information Blocking Rules will be permitted to access Network Systems under the terms of appropriate agreements, as described in Policy 21. This policy documents the criteria by which organizations may apply and become Participants in the Network. Participants have rights and responsibilities that are separate from Subscribers, which are discussed in Policy 21.

POLICY:

A Network Participant may participate as a Data Supplier, a Data Recipient, or both. A Participant may be permitted to use some, or all of the Network's services, as approved pursuant to that Participant's Agreement. To be considered for Participation in the Network, an organization must either be invited by, or apply and be approved by, the Network's Board of Directors.

ELIGIBILITY

Because access to data through the Network constitutes a disclosure of PHI from Covered Entities for permitted purposes under HIPAA and the Business Associate Agreements with Data Suppliers, Data Recipients must be organizations already accustomed to protecting the privacy and security of PHI. To this end, unless an exception is specifically granted by the Board of Directors, Data Recipients must be Covered Entities as defined by HIPAA, and neither the Data Recipient nor any of its Authorized Users may be excluded from federally funded health care programs (as identified by the United States Office of Inspector General under the U.S. Department of Health & Human Services). If Authorized users experience changes in licensure status, Authorized Administrators must review and revise their access roles, as appropriate.

APPROVAL REQUIRED

Applicants will be screened by Network Workforce for eligibility and compliance with standards of membership. Workforce will be responsible for bringing applicants to the Operations Management Committee who will make recommendation to the Board of Directors. The Board will approve or disapprove applicants as Data Suppliers, Data Recipients, both, or for other services. Applicants may be approved or disapproved individually or by rule as the Board of Directors may determine in its sole discretion, in accordance with these Policies, Business Associate Agreements, and procedures. The Network is not required to approve any application. Once an application has been approved, applicants will be notified.

ENROLLMENT

Required legal agreements, which must include agreement to these Policies, and payment terms must be signed prior to Data Recipients providing access to new Authorized Users. Data Recipients must specify their Authorized Administrators and arrange user training, in accordance with Policy 12: User Access to Systems Containing PHI. Data Recipients must also plan how they will provide patient education in accordance with the Patient Preference Policy. Network Workforce must advise Participants of their opportunities to participate in the governance structure of the Network. Network

Workforce may assist, but new Participants are responsible for establishing their Authorized Administrators, training, written materials, and other tasks required to support participation in the Network, as described in Policy 12: User Access to Systems Containing PHI.

DATA SUPPLIER CONFIGURATION

Data Suppliers are responsible to configure their systems and send only PHI that they are legally permitted to transmit. If Data Suppliers intend to supply Sensitive Information, Data Suppliers are responsible for any consent requirements, as described in Policy 3: Patient Preference.

REFERENCES:

- MyHealth Terms and Conditions Sections 4.1-4.5, 5.1, 12.3, 12.7
- Policy 3: Patient Preference
- Policy 12: User Access to Systems Containing PHI
- Policy 21: Fulfilling Requests to Access, Exchange, or Use EHI

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 2/10/2015: Initial Approval.
- 11/2/2020: Added Subscribers with a reference to Policy 21, clarifying difference with Participants.

INTEROPERABILITY WITH NON-PARTICIPANTS

POLICY 21: FULFILLING REQUESTS TO ACCESS, EXCHANGE, OR USE EHI

PURPOSE:

This policy describes how the Network will ensure compliance with the Information Blocking Rule when requests are received that constitute requests by requestors of Network as an actor, and establishes how the Network will accommodate basic data exchange under a limited license, referred to in these Policies by the term Subscriber.

POLICY:

Under the Information Blocking Rule, the Network is a "health information exchange," as that term is defined in 45 CFR §171.102, and is therefore an actor who is required to refrain from practices that constitute Information Blocking as defined under the Information Blocking Rule. A requestor may make a request for EHI from MyHealth for particular content, which is EHI, to be delivered in a particular manner, as outlined in 45 CFR §171.301 (Content and Manner Exception).

When such requests occur, Network will respond in the following ways:

If the request is already permitted under an existing Participation Agreement or Subscriber Agreement, MyHealth will fulfill the request in accordance with the terms of the applicable Agreement.

If the request is not already permitted under an existing Participation Agreement or Subscriber Agreement, then:

Network will determine if the request is allowable under the Information Blocking Rule, in accordance with the regulations in the Information Blocking Rule. Network shall establish, in consultation with Participant Suppliers, a procedure which shall be used for assessing requests. This procedure will incorporate methods for ascertaining whether the EHI being requested:

1) Meets the "Preventing Harm Exception" (45 CFR §171.201)
2) Meets the "Privacy Exception" (45 CFR §171.202)
3) Meets the "Security Exception" (45 CFR §171.203)
4) Meets the "Content and Manner Exception" (45 CFR §171.301)
5) Is addressable within the criteria allowed by the "Fees Exception" and the "Licensing Exception" (45 CFR §§171.302-303)
6) Meets the "Infeasibility Exception" (45 CFR §171.204)
7) Meets the "Health IT Performance Exception (45 CFR §171.205)

If the request for EHI meets one or more of these exceptions, Network will follow the process prescribed in the Information Blocking Rule to attempt and resolve the issues to enable Interoperability to occur.

If Network determines a request is not allowable, MyHealth will communicate this finding and the reason to the requestor, in accordance with the Information Blocking Rule.

If Network determines a request is allowable then:

Network will begin negotiation with the requestor within 10 business days from the receipt of the request, and will negotiate a license with the requestor within 30 business days from the receipt of the request, as required in 45 CFR §171.303 (Licensing Exception).

If the requestor is a Participant requesting expanded access than is currently permitted under an existing Agreement, Network will work with the Participant to incorporate the desired license under the terms of the existing Agreement, and thus addressing the request.

If the requestor is not a Participant, the license MyHealth negotiates will take the form of a Subscriber Agreement, which must be consistent with the terms of these Policies that pertain to Subscribers, and must have a means to remain consistent with these Policies when these Policies are amended. MyHealth will attempt to act in the best interests of the Network and its Participants to negotiate licenses where Subscribers also act as Subscriber Suppliers, so EHI can be exchanged bidirectionally between Subscribers and Participants.

If the requestor is requesting EHI as an Individual or for an Individual, or on the basis of an Individual's authorization, Network will respond in accordance with Policy 22: Requests for Access to Records by an Individual.

MyHealth will summarize and report on pending, new and existing Subscriber agreements to the Operations Management Committee.

REFERENCES:

- 45 CFR § 171

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 11/2/2020: Initial Approval.

POLICY 22: REQUESTS FOR ACCESS TO RECORDS BY AN INDIVIDUAL

PURPOSE:

This policy describes how Network will ensure compliance with the Information Blocking Rule when requests are received that constitute requests for EHI by an Individual, for an Individual, or on the basis of an Individual's authorization.

POLICY:

If Network receives requests for EHI for the purposes of sharing with an Individual, or for the purpose of disclosing to another party on the basis of an Individuals' authorization, Network will engage in the negotiation required by the Information Blocking Rule, and will also collaborate with Data Suppliers for the purpose of ensuring the requested EHI is not subject to one of the exceptions under the Information Blocking Rule. If Network establishes, with help of Data Suppliers, that no exceptions apply, Network will fulfill the request through the process outlined in Policy 21, Fulfilling Requests to Access, Exchange, or Use EHI.

REFERENCES:

- 45 CFR § 171

Effective Date: 11/16/2020
Latest Review Date: 2/8/2024
Revision History:

- 11/2/2020: Initial Approval.

GLOSSARY

Authorized Administrator means a Workforce member assigned in writing by a Participant to perform the corresponding duties and functions outlined in the Policy 12: User Access to Systems Containing PHI.

Authorized User means an individual who has been authorized by a Participant or Subscriber to access PHI via the Network.

Breach has the same meaning as the term "Breach" as defined in 45 CFR § 164.402, as it may be amended from time to time.

Business Associate has the same meaning as the term "Business Associate" as defined in 45 CFR § 160.103. With regard to PHI, the Network functions as a Business Associate of its Participants.

Business Associate Agreement means a written signed agreement meeting the HIPAA requirements in 45 CFR § 164.504(e). The MyHealth Participation Terms and Conditions which are incorporated into Network Agreements are Business Associate Agreements.

Covered Entity has the same meaning as the term "Covered Entity" as defined in 45 CFR § 160.103.

Cures Act means the 21st Century Cures Act (codified at 42 USC § 300jj-52) and the regulations promulgated thereunder (including the Information Blocking Rule, found in 45 CFR Part 171), any amendments thereto.

Data Recipient means a Participant Recipient or a Subscriber Recipient who accesses or receives PHI from the Network. This term is used for instances in which the entity's status as a Participant or Subscriber is not important to the use of the term.

Data Supplier means a Participant Recipient or a Subscriber Recipient who accesses or receives PHI from the Network. This term is used for instances in which the entity's status as a Participant or Subscriber is not important to the use of the term.

De-identified Data means data that has been stripped of all identifiers in accordance with HIPAA in 45 CFR § 164.514(a)-(c) as well as source identity.

Electronic Health Information ("EHI") has the same meaning as the term "Electronic Health information" as it is defined and used in the Information Blocking Rule (45 CFR § 171).

Individual means the person who is the subject of the PHI, as defined in 45 CFR § 160.103, and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

HIPAA means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder at 45 CFR Parts 160, 162, and 164 and any amendments thereto.

HITECH means the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A of the American Recovery and Reinvestment Act of 2009, and the regulations promulgated thereunder and any amendments thereto.

Information Blocking Rule means the regulation promulgated under the Cures Act in 45 CFR Part 171, and any amendments thereto.

Limited Data Set means PHI that excludes all direct identifiers of an Individual or of all relatives, employers, or household members of the Individual that are required to be removed pursuant to 45 CFR §164.514(e).

Network means MyHealth Access Network, Inc., which is the organization that oversees the technology infrastructure of MyHealth Access Network.

Network Agreement means either the MyHealth Participation Agreement and its incorporated documents.

Network System means the technology infrastructure that enables the exchange of PHI. This term refers to the technology infrastructure of MyHealth Access Network.

MyHealth means MyHealth Access Network, Inc., or the technology platform which bears its name, depending on the context of usage.

NIST means the National Institute of Standards and Technology.

Participant means a Provider Organization, Payer Organization, or Practitioner that has directly or indirectly entered into a Network Agreement with the Network and supplies (a "Data Supplier") or accesses (a "Data Recipient") PHI via the Network.

Participant Recipient means a Participant who accesses PHI via the Network.

Participant Supplier means a Participant who provides PHI to the Network.

Policies means this document. When not capitalized, this word refers generically to the provisions that may be contained in this document, or in other policy documents, based on context.

Protected Health Information ("PHI") has the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the individually identifiable health information created or received by a Business Associate from or on behalf of a Covered Entity. This term includes Electronic Protected Health Information ("EPHI"), which is further defined as PHI that is transmitted by "electronic media" (as that term is defined at 45 CFR § 160.103) or that is maintained in any form of electronic media.

Secretary means the Secretary of the United States Department of Health and Human Services.

Sensitive Information means any information subject to special privacy protection under state, federal, or other applicable law, including but not limited to psychotherapy notes and drug or alcohol abuse treatment records, or any other PHI that may require explicit patient consent for disclosure. In some jurisdictions this may include HIV/AIDS, communicable disease, mental health, reproductive health, sexually transmitted disease, and/or genetic testing information.

Subcontractor Business Associate Agreement means a written signed agreement between the Network and a subcontractor which meets the HIPAA requirements of a Business Associate Agreement, and as applicable, which incorporates the obligations of the Network under its Network Agreements and these Policies.

Subscriber means an entity who makes a request for Electronic Health Information, as defined in the Information Blocking Rule, to the Network (thus making Network the actor under the Information

Blocking Rule), and enters into a Subscriber Agreement with the Network which incorporates terms consistent with those in these Policies as they pertain to a Subscriber. Subscribers may become contributors of PHI to the Network, as long as the Subscriber Agreement incorporates compatible terms such that Data Recipients can utilize PHI contributed by Subscribers with no greater restrictions than the ways in which they can utilize PHI contributed by other Data Suppliers.

Subscriber Agreement means an agreement between a Subscriber and the Network which incorporates the terms from these Policies as they pertain to the Subscriber.

Subscriber Recipient means a Subscriber when that Subscriber is acting in the capacity of a requestor of EHI from the Network as defined in the Information Blocking Rule, under the terms of a Subscriber Agreement.

Subscriber Supplier means a Subscriber when that Subscriber is submitting EHI to the Network voluntarily, or when that Subscriber is acting in the capacity of an actor, in responding to a request for EHI in an exchange where the Network is the requestor, as these transactions are described in the Information Blocking Rule, and under the terms of a Subscriber Agreement.

Workforce means employees, students/trainees, volunteers, contractors, and other individuals under the direct control of a Participant or of the Network (depending on context), whether or not they are paid and whether or not their involvement is temporary or long-term.