GOVERNING POLICIES

Health Information Exchange and Community Resource Network

July 12, 2023

CONFIDENTIAL

Marc Lassaux
Executive Director and CEO
mlassaux@qualityhealthnetwork.org
Richard Warner
CISO/Chief Project Officer
rwarner@qualityhealthnetwork.org
Janet Terry
Privacy and Compliance Officer
jterry@qualityhealthnetwork.org
Kurt Bergstrom
Security Officer
kbergstrom@qualityhealthnetwork.org

744 Horizon Court, Ste. 210
Grand Junction, CO 81506
Phone: 970-248-0033

TABLE OF CONTENTS

INTRODUCTION AND DOCUMENTS INCORPORATED BY REFERENCE

The following Policies of Quality Health Network ("QHN") establish requirements that must be followed by Quality Health Network, Participants, Participant Users, QHN's officers, directors, employees, subcontractors, agents, and contracted organizations, and any person who accesses the QHN System. These Policies apply to both the HIE and CRN, unless otherwise stated in a particular Policy.

These Policies are to be interpreted, applied and enforced by QHN in its sole discretion and in furtherance of the mission of QHN. QHN may waive a specific Policy requirement, when appropriate under the circumstances and permitted by applicable law; provided that a waiver in one instance shall not be considered a general waiver of any particular requirement or in any other instance.

These Policies are incorporated and made part of the "QHN Standards" which are referenced in the Electronic Commerce Agreement between QHN and Participants. Through the Electronic Commerce Agreements, Participants have agreed to Use the QHN System in a manner consistent with and to comply with QHN's Standards and applicable law. Changes to these Policies may reflect changes in applicable law or the need to adopt new technologies, systems, or desired functionality or changes in QHN's operational procedures. Participants are encouraged to provide input regarding these Policies and to propose changes.

DEFINITIONS

Terms used but not otherwise defined in the Quality Health Network ("QHN") Policies shall have the same meaning as those terms defined in HIPAA, when applicable. All terms defined in these QHN Policies shall be interpreted and read to have a meaning consistent with terms defined in HIPAA. Capitalized terms in these QHN Policies are defined as follows:

1) "Board of Directors" shall mean the Board of Directors of QHN.

2) "Care Coordination" shall mean the planning and coordination of patient care among health care providers which may also include coordination of related services provided by social service organizations, and coordination of social services among non-Covered Entities, to facilitate delivery of health care, social services or other resources that may be needed by an individual. If the "Care Coordination" involves the Disclosure of PHI, then a Disclosure may only occur if it is permitted by HIPAA or with Individual authorization in the form of CRN Consent.

3) "Community Resource Network" (or "CRN") shall mean the system operated by QHN to facilitate the exchange of Records among Participants.

4) "Community Services Information" or "CSI" shall mean information created, maintained, or received by a public, governmental or private entity, including information that relates to the past, present or future need for or provision of services related to an Individual. CSI is information which is not subject to the requirements of HIPAA.

5) "Covered Entity" shall mean a person or entity that meets the definition of a Covered Entity under HIPAA, and generally includes health care providers, health plans and health care clearinghouses.

6) "De-identification" or "De-identified" shall mean to remove, encode, encrypt, or otherwise eliminate or conceal data which identifies an Individual, or modifies information so that there is no reasonable basis to believe that the information can be used to identify an Individual. De-identification includes, without limitation, any process meeting the requirements for De-identification set forth in 45 C.F.R. § 164.514, as such provision is currently drafted and as it may be subsequently updated, amended, or revised.

7) "Disclosure" or "Disclose" means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

8) "DURSA" shall mean the Data Use and Reciprocal Support Agreement between QHN and the eHealth Exchange.

9) "DURSA Participant" shall mean any organization that meets all of the requirements for participation in the eHealth Exchange as specified in the DURSA.

10) "eHealth Exchange" shall mean the public-private partnership which was formerly known as the Nationwide Health Information Network ("NwHIN").

11) "Executive Director" shall mean the Executive Director of QHN or such Executive Director's designee.

12) "Health Information Exchange" or "HIE" shall mean the system operated by QHN primarily to facilitate the exchange of PHI among HIPAA Covered entity Participants, their business associates, and for purposes allowed by HIPAA.

13) "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, as amended and including any implementing regulations ("HIPAA"), including specifically 45 C.F.R. Parts 160 and 164.

14) "Individual" shall mean a natural person who is the subject of PHI or CSI.

15) "Information Privacy Laws" shall mean(a) the Health Insurance Portability and Accountability Act of 1996, as amended and including any implementing regulations ("HIPAA"); (b) Health Information Technology for Economic and Clinical Health Act in the American Recovery and Reinvestment Act of 2009, including any implementing regulations ("HITECH") any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy or security of information pertaining to an Individual, (c) any other statute, regulation, administrative or judicial ruling requiring a party to protect the confidentiality, privacy and/or security of information pertaining to Individuals; all to the extent that such Information Privacy Laws have been enacted, promulgated, issued or published by any federal or state governmental authority with jurisdiction over a Covered Entity, a Business Associate, an Individual, Participant or QHN.

16) "Opt Out" shall mean that access to an Individual's Records in the QHN System is restricted as provided by these Policies.

17) "Participant" shall mean any person or entity which QHN has agreed to accept for enrollment, which desires to access the QHN System provided by QHN for the purpose of promoting the improvement of health care treatment, payment, health care operations or coordination of community services, pursuant to an Electronic Commerce Agreement entered into with QHN.

18) "Participant User" shall mean any person who is authorized to use the QHN System through Participant's right of Use set forth in a Participant's Electronic Commerce Agreement. Participant shall identify those persons it wishes to designate as Participant Users. QHN has the ability to add or remove a person's right to use the QHN System. Participant Users shall be natural persons.

19) "Permitted Purposes "shall mean the reasons for which Participants and Participant Users may use the QHN System, and includes the Use and Disclosure of Records for purposes of: (a) Treatment, Payment and Health Care Operations (as those terms are defined in HIPAA), (b) quality improvement programs, (c) health care coordination and service coordination, (d) Uses and Disclosures permitted by an authorization or consent meeting requirements of applicable laws including but not limited to Information Privacy Laws, and (e) for such other purposes described in QHN Standards as may be allowed by applicable law.

20) "Procedures" shall mean those procedures adopted by QHN to implement Policies.

21) "Protected Health Information," or "PHI," shall have the meaning as the term "protected health information" in 45 C.F.R. 160.103 and 164.501.

22) "QHN Policies" or "Policies" shall mean these governing Policies of QHN, as they may be amended or added to from time to time.

23) "QHN Standards" or "Standards" shall mean those standards, Policies and procedures adopted by QHN, which address requirements and standards with regard to Use of the QHN System. QHN's Standards may address and include, but are not limited to: activity on the QHN System, operating rules, definitions and specifications of format, content, and transmission of electronic data, support descriptions and details of connecting to the QHN System.

24) "QHN System" or "System" shall mean the technology tools, services and information storage and computing systems QHN provides and/or maintains for Use by Participants, and includes, but is not limited to the HIE and CRN.

25) "Records" as used in these Policies shall refer to both PHI and CSI, in any form or format; a particular record may in certain circumstances only include PHI or CSI.

26) "Subscription Services" shall mean those services which allow a Participant to receive those portions of an Individual's Records that have been identified to such Individual and transmitted through the QHN System.

27) "Use" shall mean the access to, sharing, employment, application, utilization, examination, analysis, De-identification, or commingling of PHI or CSI with other information, within an entity that holds the information.

28) "Users" shall mean collectively QHN, Participants and Participant Users authorized to Use the QHN System.

	Section 1: System Access and Use
Policy 1.0	**STANDARD**
	Participant Enrollment: A Participant shall be required to complete QHN enrollment processes and E-Commerce Agreements before a Participant or Participant User may access and use the QHN System.
	POLICY
QHN Determines Enrollment Standards	1) Participants and Participant Users shall complete enrollment materials, including but not limited to confidentiality agreements or attestations required by QHN before access is granted to the QHN System.
Participants Designate Participant Users	2) The Participant will designate, in a form acceptable to QHN, all proposed Participant Users whom the Participant desires to have access rights to the QHN System.
Changes in Participants Users Access	3) Participant shall notify QHN of any changes in the status of a Participant User's access rights to the QHN System.
Unauthorized System Access	4) Unauthorized use of the QHN System may result in sanctions, which may include civil damages as well as criminal prosecution.
QHN May Deny Access	5) Notwithstanding any other provision of QHN Policies, QHN, in its sole discretion, (a) may deny any applicant's request to become a Participant and/or a request for a Participant Users access rights to the QHN System or(b) may deny, suspend, modify, or terminate access rights or ability of any person or entity, including any Participant or Participant User, to the QHN System. When exercising this discretion, QHN may consider various factors including but not limited to, the Participant's or Participant User's credentials, licensure, security policies and practices, physical location (e.g., whether information will be accessed from outside the United States) or other information.
Notify QHN of Termination	6) As soon as reasonably possible following termination of a Participant User's relationship with Participant (e.g.: termination of employment), Participant will take steps to disable the Participant User's access rights and will also notify QHN of such termination.

Notify QHN of Status Change	7) Each Participant shall notify QHN of any loss of privileges with Participant, loss or suspension of health care provider licensure or termination of employment of any Participant User who is granted access to the QHN System. In such event Participant User's access to the QHN System through Participant shall be terminated, except as otherwise may be approved in writing by QHN.
Fees Assessed by QHN	8) Notwithstanding any provision of QHN's Policies, E- Commerce Agreement or other agreements, QHN in its sole discretion reserves the right to require additional conditions be met as QHN deems appropriate for any granted use of the System. 9) Participants shall pay the applicable fees, as required by QHN, for Participant's use of the QHN System. QHN reserves the right to refuse or terminate access if payment is not received.
Policy Dates	Written: August 25, 2005 Amended: September 15, 2010; February 28, 2014 (DT); February 10, 2016; July 28, 2020; July 12, 2023September 15, 2010; December 21, 2011; February 28, 2014 (DT); February 10, 2016; July 28, 2020; July 12, 2023. Reviewed:

Policy 1.1	STANDARD
	Participant Training: Participants must comply with applicable laws and QHN requirements concerning training of their Participant Users.
	POLICY
Training Required Compliance with QHN Standards Participant to Document Training	1) Before accessing the QHN System, each Participant User must receive training, as required by this Standard and applicable law. 2) All Participants that are HIPAA Covered Entities or HIPAA Business Associates are required to provide HIPAA privacy and security training for all Participant Users. 3) QHN may require CRN System Participant Users to complete required training regarding confidentiality laws and consequences for misuse of the CRN System. 4) By use of the QHN System, each Participant User agrees to comply with QHN Standards and all applicable laws. Participants are encouraged to attend training for proper use of the QHN System. 5) Upon request, Participant will provide attestation or documentation of such training to QHN.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 1.2	STANDARD
	Role Based Access: All Participant Users are granted access to the QHN System in a manner that is consistent with their roles and job duties, and in accordance with all applicable laws.
	POLICY
Access Level Determined by QHN	1) Participant Users will be assigned a level of system access, based upon their roles and job duties. Participants will only request access for those persons who need to access Records to carry out their roles and duties and such access shall be established at a level that takes into account the categories and types of PHI or CSI needed and any conditions appropriate to such access.
QHN Approves any Change in Access	2) QHN will determine if QHN or Participant will establish the level of QHN System access for a Participant User. QHN may establish the roles from which a Participant may choose. 3) QHN may require Participants to attest that the access level or role and job duties assigned to a Participant User is in accordance with QHN Standards and applicable law. At its discretion, QHN may audit and change a Participant User's level of access to the QHN System.
Policy Dates	Written: August 25, 2005 Amended: August 14, 2013; February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; August 14, 2013; February 10, 2016; July 28, 2020; July 12, 2023

Policy 1.3	STANDARD
	Participant Use of QHN System: Use of the QHN System by a Participant and all Participant Users must be in compliance with all applicable laws and consistent with QHN Standards
	POLICY
Use of QHN System	1) Use of the QHN System by Participants and Participant Users, must be in compliance with Permitted Purposes and in compliance with Participant's Electronic Commerce Agreement, QHN Standards and applicable law.
Participant's Responsibility	2) Inappropriate use of or access to the QHN System by any Participant User may result in all Participant Users losing the right to access the System and the imposition of sanctions, as identified in these QHN Policies. If the Participant at any time finds that the Participant User's access has not been appropriate, Participant shall immediately:
Notification of Inappropriate Access	A. Terminate all such Participant User's access to the QHN System from within Participant's system, and B. Notify QHN, at which time, QHN will remove all access rights to the QHN System for the Participant User.
QHN May Report	3) QHN may report any inappropriate use of or access to the QHN System by a Participant User to the appropriate agencies with whom the Participant User is licensed and/or to other agencies or organizations with whom a Participant User has a relationship or privileges that are likely to allow the Participant User to have access to Records.
Notification Costs Paid by Participant	4) If QHN is required by law to provide notifications to any Individual(s), other Participants and/or any governmental entity of inappropriate use of or access to the System by a Participant User or any person who accesses the System through Participant's right of access or take other action, the Participant

Sanctions for Misuse	shall pay all QHN's costs and expenses including all costs of investigating and mitigating any harmful effects caused by the inappropriate access. 5) Any Use of the QHN System by QHN, a Participant or Participant User that is contrary to QHN Policies Standards, Electronic Commerce Agreements, and any applicable law, regulation or government policy, is prohibited. Sanctions related to restricting or terminating QHN System access and use may be imposed, at the sole discretion of QHN, on Participants or Participant Users who use the QHN System or data or information in the QHN System in violation of this policy. In addition, Participants will be liable for damages caused by misuse.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016; July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 1.4	STANDARD
	Participant System Security Requirements: Each Participant shall maintain appropriate administrative, physical and technical safeguards, in accordance with applicable law, for its own computing systems that are reasonably designed to protect the confidentiality, integrity and availability of Records in the QHN System.
	POLICY
System Requirements	1) Each Participant is responsible for maintaining the minimum required equipment, technology and processes, in order to achieve optimal and secure access and use of the QHN System. 2) QHN may require a documented attestation from a Participant that the systems used to access the QHN System are in compliance with HIPAA and other applicable law.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016; July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 1.5	STANDARD
	Participants and Participant Users Responsible for Accurate Delivery of Records: Participant and Participant Users are responsible for notifying QHN of current routing information in order to assure accurate and appropriate delivery of Records
	POLICY
Participant Users Responsible for Accurate Delivery	1) Participants and Participant Users are responsible for notifying QHN and all applicable data sources (e.g., hospital, labs, and other entities that place results in the System) as to accurate and current work and practice location(s) of Participant Users, including any changes or additions regarding practice locations. 2) Participant Users who work at multiple practice locations shall ensure that Records will be maintained and Used in compliance with all applicable laws.
Policy Dates	Written: April 17, 2013 Amended: February 10, 2016: July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 1.6	STANDARD
	Participant Notice to Individuals about HIE Participation: Each health care provider Participant shall provide Individuals with a notice regarding Participant's use of the HIE to Use and Disclose PHI and the Individual's ability to Opt Out.
	POLICY
Notice about participation in the HIE. Format May be Electronic.	1) Each health care provider Participant shall provide all Individuals who are patients of the Participant with a written notice ("Notice") (a) that the Participant uses the HIE to Use and Disclose PHI regarding the Individual and (b) that the Individual has the right to request to Opt Out. (Note: For more information regarding Opt Out, please see Policy 10.) 2) The Notice may be incorporated in the Participant's Notice of Privacy Practices that is provided as required by HIPAA or other format, including by electronic means, as deemed appropriate by the Participant. 3) Participants shall provide copies of the Notice used by Participant and documentation to demonstrate that the Notice is provided to Individuals, as required under this Standard, within five (5) business days of a request by QHN for such information. 4) Sample language that a provider may utilize for the Notice is included at the end of these Governing Policies as Supplemental Information.
Policy Dates	Written: July 12, 2023 Amended: _____ Reviewed: July 12, 2023

	Section 2: Subcontractor/Agent/Other Contracted Organizations
Policy 2.0	**STANDARD**
	System Access, Workforce Clearance and Security Requirements: Any subcontractor, agent, or other organization who will have access to the QHN System shall agree with and be bound by applicable restrictions and conditions regarding Use of the QHN System that apply to QHN including Electronic Commerce Agreements, Business Associate Agreements to which QHN is a party and all applicable laws.
	POLICY
Agreement Required	1) QHN shall require subcontractors, agents or other organizations who will have access to the QHN System to enter into confidentiality agreements that are compliant with applicable law and that prohibit use or disclosure of Records other than is allowed by applicable law.
	2) Any agreements that permit PHI access, will contain at least the same restrictions and conditions applying to QHN in any Business Associate Agreement or other agreements to which QHN is a party.
	3) Subcontractors, agents or other contracted organizations will not have access to the QHN System until such agreement is fully executed.
Possible Sanctions	4) Failure or alleged failure of a QHN subcontractor, agent or other contracted organization to comply with QHN Standards or any written agreement with QHN may result in an investigation and possible sanctions.
Responsible for Damages	5) Subcontractors, agents or other contracted organizations shall be responsible for all damages to QHN, occurring as a result of misuse of the QHN System.
Background Checks Required	6) Prior to any subcontractor, agent or other contracted organization providing services related to the QHN System, QHN may require that such organizations conduct background checks on employees of subcontractor, agent or contracted organization who may have more than incidental access to Records in the QHN System.
System Security is Compliant	7) Subcontractors, agents or other contracted organizations that are providing managed hosting, software, and/or other technological services related to the QHN System shall maintain administrative,

	physical and technical safeguards required by applicable federal and state law, and QHN Policies.
Compliant with Law and Safeguards in Place	8) Every subcontractor, agent or other contracted organization shall maintain privacy and security policies and/or standards as required by applicable federal and state law, and QHN Standards. 9) Every subcontractor, agent or other contracted organization shall ensure that, prior to accessing the QHN System, any employee who will access the QHN System will: a) Hold all Records on the QHN System confidential; b) Hold all QHN proprietary information confidential; and, c) Have completed HIPAA Privacy and Security Training if they will have access to PHI.
Security Audits Upon Request	10) Upon request by QHN, every subcontractor, agent or contracted organization shall work with QHN to provide assurance that all accesses to the QHN System by any members of their workforce are in compliance with HIPAA if they will have access to PHI, all federal and state laws, and QHN Standards
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

	Section 3: System Access – Non Participant
Policy 3.0	**STANDARD**
	System Access by Special Agreement: Access to and Use of the QHN System by organizations and users which are not Participants or Participant Users is by special agreement entered into directly with QHN.
	POLICY
QHN Determines Agreement	1) QHN may grant access to, and Use of the QHN System to organizations that may not meet the definition of a Participant, such as, but not limited to, other health information exchange organizations, care coordinators, or allied health organizations. 2) Such access shall be defined by special agreement acceptable to QHN. 3) Any special agreements for access to and Use of the QHN System will comply with HIPAA, all applicable federal and state laws, QHN Standards and any privacy and security requirements established by QHN.
Policy Dates	Written: February 10, 2016 Amended: _____ Reviewed: July 28, 2020; July 12, 2023

	Section 4: Passwords/User ID/User Workstation
Policy 4.0	**STANDARD**
	Unique User ID and Passwords Required: Every QHN System User is required to have a unique User ID and password in order to access the QHN System. QHN will set the configuration standards for the User ID and password.
	POLICY
Standards Determined by QHN User Creates Unique Password QHN May Disable User ID and Password	1) As used in this Section 16, the term "User" shall mean Participant Users, QHN employees, contractors and vendors and any other person granted access to the QHN System. 2) Each User shall have a unique User ID and password/authentication. Such User ID and password/authentication shall be established and maintained in accordance with QHN Standards. 3) Users are responsible for creating and securing their unique password. 4) Users are not allowed to share their unique User ID or password. Users are responsible for activity associated with the use of their unique User ID and password. 5) If a User suspects that their password has been compromised, the User shall immediately reset their password and notify QHN. 6) QHN retains the right to disable the User ID and password if QHN determines that inappropriate use of the System has occurred or is suspected. 7) Misuse of a User ID or password may result in Sanctions being imposed by QHN, as outlined in these Policies and the QHN Employee Handbook.
Policy Dates	Written: August 25, 2005 Amended: December 21, 2011; February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 4.1	STANDARD
	Single Sign On User ID: Each User who will utilize Single Sign On to the QHN System shall use a unique log-in ID and unique password for access to the QHN System in compliance with QHN Standards.
	POLICY
Unique Log In ID Single Sign On Attestation	1) Single Sign On functionality provides the ability for the Participant or Participant User to log in directly to the QHN System from the Participant's electronic system. Use of Single Sign On must be approved by QHN and will only be approved if Participant confirms that Participant's Single Sign On functionality is at least as secure as the QHN System login, access and related security requirements. 2) An attestation or agreement in a form acceptable to QHN may also be required for use of Single Sign On functionality.
Policy Dates	Written: April 17, 2013 Amended: February 10, 2016 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 4.2	STANDARD
	Secure Workstation: Each User shall maintain physical control of the workstation, including laptop computers or mobile devices, used for access of the QHN System
	POLICY
System Timeout User Workstation Security	1) Access to the QHN System for a session is terminated when the User either logs out or the system timeout has been activated. 2) Each User is responsible for securing their workstation in accordance with HIPAA and these QHN Policies so as to prevent unauthorized access to the QHN System.
Policy Dates	Written: December 21, 2011 Amended: _____ Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

	Section 5: Impermissible Use or Disclosure of Records/Breach Notification
Policy 5.0	**STANDARD**
	Participant Notice to QHN: A Participant is required to notify QHN should Participant suspect that an impermissible Use or Disclosure of Records, related to use or access of the QHN System, has occurred.
	POLICY
Notice to QHN	1) Participant will notify the QHN Privacy/Security Officer or Executive Director, as soon as reasonably possible after becoming aware of any impermissible Use or Disclosure of Records, related to use or access of the QHN System.
	2) Participant shall, as part of the notification, inform the QHN Privacy/Security Officer or Executive Director as to the facts surrounding the impermissible Use or Disclosure of Records. Participant shall inform QHN of procedures taken to remedy the problem.
QHN Hold Harmless	3) Participant shall indemnify and hold QHN harmless from any claim, demand, or suit alleging improper Use or Disclosure of Records in any way related to Participant's use of or access to the QHN System. This indemnity shall include, but is not limited to the payment to QHN for attorney's fees, court costs and expert witness fees QHN incurs in defending itself from any such claim, demand, or suit.
Participant Responsible for Compliance	4) Except as provided by these Policies and E-Commerce Agreements, QHN shall not be responsible for compliance with any laws, regulations or other requirements that may apply to the Records. Participants will be solely responsible for compliance with any laws, regulations or other requirements that may apply to such Records.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 5.1	STANDARD
	QHN Investigation of Use or Disclosure/Notice to Participant: Upon discovery by QHN of an impermissible Use or Disclosure of a Records related to use of the QHN System, the QHN Privacy and Security Officer shall conduct a prompt investigation and report findings to the Executive Director.
	POLICY
Notice to QHN Privacy/Security Officer	1) Any QHN employee, agent, representative or subcontractor who discovers or learns of a potential impermissible Use or Disclosure of a Record related to use of or access to the QHN System will notify the QHN Privacy/Security Officer as soon as reasonably possible.
QHN to Investigate	2) After receiving notification of an impermissible Use or Disclosure of a Record the QHN Privacy/Security Officer shall conduct a prompt investigation. If PHI is involved, then the QHN Privacy/Security Officer shall also follow applicable requirements of HIPAA and any applicable E-Commerce Agreements.
Notice to Executive Director	3) The QHN Privacy/Security Officer shall, as soon as is reasonably possible, notify the Executive Director of the reported potential impermissible Use or Disclosure of Records. Upon conclusion of the investigation, the QHN Privacy/Security Officer shall inform the Executive Director of the findings and outcome of the investigation.
Notice to Board of Directors	4) The Board of Directors will be notified as determined by the Executive Director.
Notice to Participant	5) QHN will notify the Participant(s) involved promptly after QHN has knowledge of an impermissible Use or Disclosure. Such notification shall be made in accordance with applicable law and any agreement to which QHN is a party.
Breach Notification	6) Should QHN determine that a Breach, as defined by HIPAA, has occurred, QHN shall give notice, in accordance with applicable law and any agreement to which QHN is a party.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

	Section 6: Data Integrity
Policy 6.0	**STANDARD**
	Information Standards: Information shall be submitted to the QHN System in a form that is acceptable to QHN in accordance with the standards developed by QHN.
	POLICY
Information to Comply with QHN Standards	1) All information placed in the QHN System shall comply with QHN Standards for placement of information in the QHN System. 2) The data that is placed in the QHN System by or on behalf of a Participant who is a Covered Entity, shall be for the purposes of treatment, payment and health care operations as defined by HIPAA. Data that is placed in the CRN System shall be for coordination of community services, including the coordination of community services with health care services.
Participant Responsible for Accuracy of Data	3) Participant is solely responsible for the accuracy of Records and data placed in or transmitted by or on behalf of Participant or Participant Users in the QHN System. 4) QHN disclaims any warranty or representation as to the accuracy or completeness of Records and data within the QHN System. Participant and Participant Users are responsible for verifying the accuracy and completeness of Records or data Used or relied upon.
Possible Sanctions	5) Sanctions may be imposed, at the sole discretion of QHN, on Participants or Participant Users who place data into the QHN System in violation of this policy.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

	Section 7: Records Subject to Special Protections
Policy 7.0	**STANDARD**
	Participant Responsibility: All Participants and Participant Users who use the QHN System will comply with provisions in applicable law governing access to Records containing information about certain conditions or services which are subject to special protections, standards or confidentiality requirements.
	POLICY
Knowledge of privacy laws	1) Each Participant or Participant User shall be aware of applicable laws that create or impose special protections, standards or confidentiality requirements for certain Records. Examples of such Records include but are not limited to: alcohol and substance use disorder treatment records, psychotherapy records, records involving HIV diagnoses, records regarding minors and other records subject to special protection.
Participant Responsibility	2) When entering or facilitating addition of Record information into the QHN System, the Participant or Participant User shall be solely responsible for taking appropriate precautions regarding accessing Record in the QHN System about certain conditions which are subject to special privacy standards or confidentiality requirements. Participant shall not use the QHN System in a way that does not comply with applicable law. QHN shall not have the responsibility for limiting access to such Records, unless provided for by these Policies or separate agreement.
QHN Hold Harmless	3) Participant shall indemnify and hold QHN harmless from any claim demand or suit alleging improper access or Use of Records related to medical conditions, diagnoses, treatment, CSI, or other services that are subject to special protections, standards or confidentiality requirements. This indemnity shall include but is not limited to the payment to QHN for attorney's fees, court costs and expert witness fees QHN incurs in defending itself from any such claim, demand, or suit.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

	Section 8: Participant Subscription Services
Policy 8.0	**STANDARD**
	Subscription Services: QHN may provide Participants that are Covered Entities, with Subscription Services for Individuals with whom Participant has a treating relationship for purposes of "treatment," "payment" or "health care operations" activities, as defined by HIPAA.
	POLICY
Execution of Agreement	1) Participant shall agree to the terms and conditions established by QHN prior to QHN providing Subscription Services to Participant.
Participant Required to Notify QHN of Changes	2) Participant is responsible for maintaining an accurate record of all Individuals for whom Subscription Services are provided and for enabling and/or disabling the Subscription Services within the QHN System for a particular Individual. 3) Subscription Services for a Participant may include extraction of an Individual's Records, as directed by the Participant. Participant must notify QHN of any changes to those subscribed Individuals when Subscription Services are no longer needed because Participant no longer has a treating relationship.
QHN Hold Harmless	4) Participant shall indemnify and hold QHN harmless from any claims, penalties, costs or damages (including attorney's fees) arising out of or related to Participant's use of Subscription Services or Participant's failure to comply with the terms of this policy and the agreement referenced in paragraph 1 above.
Subscription Excludes Opt Out and Specially Protected Records	5) Subscription Services for a Participant may exclude Records of an Individual who has chosen to Opt Out of the QHN System. 6) Subscription Services for a Participant may exclude Records that are governed by special privacy standards or confidentiality requirements that restrict the disclosure of such Records. 7) This Policy shall not prohibit QHN from entering into agreements to provide access to Records in a manner that is not addressed in this Policy as allowed by law.
Policy Dates	Written: February 10, 2016 Amended: _____ Reviewed: July 28, 2020; July 12, 2023

	Section 9: Records – Individual Rights
Policy 9.0	**STANDARD**
	Access to Records: Participant will allow Individuals, or a person with appropriate authority to act on an Individual's behalf, to have access to Records as required or allowed by HIPAA or other applicable laws. QHN should refer requests for access to Records to the appropriate Participant; however, requests for access to Records may be handled by QHN in its sole discretion.
	POLICY
Requests Made to QHN by an Individual	1) If an Individual requests that QHN provide access to the Individual's Record in the QHN System, or if a person with appropriate authority to act on an Individual's behalf requests such access (i.e., a personal representative or pursuant to a valid HIPAA authorization), QHN may either handle the request by providing the appropriate Records or direct the Individual to submit the request to the appropriate Participant.
Policy Dates	Written: July 28, 2020 Amended: _____ Reviewed: July 28, 2020; July 12, 2023

Policy 9.1	STANDARD
	Amendments to Records: Participant may make amendments to Records as required or allowed by HIPAA or other applicable laws. QHN will refer any Individual requests for Amendment to PHI to the appropriate Participant. If an Individual requests an amendment to CSI maintained in the CRN system, then QHN may choose to make the amendments, or request that the Participant make the amendment.
	POLICY
Requests Made to Participant by an Individual QHN's Role Participant's Role QHN Not Responsible for Amendments	1) If an Individual requests an amendment to the Individual's Record in the QHN System QHN will generally forward the request to the Participant; however, basic requests to amend CSI may be handled by QHN. 2) If an Individual makes a request to QHN related to an Individual's Records in the QHN System, the Individual will, in most cases, be informed that QHN does not handle such requests from Individuals, and the Individual will be directed to make the request to the appropriate Participant. QHN will notify the appropriate Participant (generally the Participant that submitted the particular Record for inclusion in the QHN System) within 5 business days, if QHN receives such a request from an Individual. However, if the request is limited to a basic amendment to CSI, such as to correct or update demographic information, QHN may handle the request. 3) If the Participant has agreed to make the requested amendment to the Record, Participant shall then submit the amended Record to QHN. 4) QHN shall not be responsible for the accuracy of any amendments made to Records by Participants.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016, July 28, 2020 Reviewed: December 21, 2011; February 10, 2016, July 28, 2020; July 12, 2023

Policy 9.2	STANDARD
	Accounting of PHI Disclosures: QHN will provide information to a requesting Participant, to enable the Participant to respond to a request by an Individual for an accounting of disclosures of PHI as required by law. This policy does not apply to CSI.
	POLICY
QHN Record of Disclosure	1) If QHN makes a disclosure of PHI that requires an accounting of disclosure under HIPAA, QHN shall maintain an accounting or record of such disclosures as may be required by HIPAA and applicable law. HIPAA generally requires the accounting of all disclosures of PHI, when the disclosure is not for Treatment, Payment or Health Care Operations (as defined in HIPAA), to the individual, or pursuant to a valid HIPAA authorization.
Accounting to the Participant from QHN	2) Upon receipt of a written request from a Participant for an accounting of disclosures of PHI, QHN will provide to the Participant an accounting in compliance with HIPAA and any business associate agreements to which QHN is a party.
Participant Responsibility	3) The Participant is responsible for providing the Individual with the accounting prepared by QHN in accordance with requirements of HIPAA.
	4) If an Individual makes a request to QHN for an accounting of disclosures related to PHI in the QHN System, the Individual will be informed that such requests must be made directly to the appropriate Participant.
	5) QHN will notify Participant within 5 business days, if QHN receives such a request from an Individual.
Fees Consistent with HIPAA	6) Consistent with HIPAA, QHN will not assess the Participant a fee for the first accounting of disclosures of PHI request made within a twelve (12) month period or the then current timeframe provided by HIPAA; however, for any additional requests during such period and as permitted by applicable law, QHN reserves the right to assess a reasonable cost based fee after first advising the Participant of the fee.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016, July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 9.3	STANDARD
	Recording Access to PHI and List of Access: Upon receipt of a request from an Individual, Participant may request that QHN provide information to Participant as to access to an Individual's PHI within the QHN system for the purpose of allowing the Participant to respond to an Individual's request for a list of accesses to the PHI, including accesses for treatment, payment and health care operations, as required by applicable law. QHN will respond to an Individual's requests for a list of access to PHI, as required by applicable law.
	POLICY
Requests made to a Participant by an Individual	1) Upon receipt of a request from an Individual for a list of accesses to the Individual's PHI, Participant shall submit the request to QHN, in accordance with QHN Procedures in place at that time.
	2) QHN will notify Participant within 5 business days if QHN receives a request from an Individual for a list of accesses to the Individual's PHI.
QHN's role	3) QHN will make a good faith effort to provide the list of accesses as required by applicable law which is currently for a period of three (3) years prior to the date on which the request is made. QHN will not assess a fee for the first requested list of accesses made within a twelve (12) month period or the then current timeframe provided by law; however, for any additional requests during such period and as permitted by applicable law, QHN reserves the right to assess a reasonable cost based fee after first advising the Individual of the fee and permitting the Individual to withdraw the request.
Denial and Expenses	4) QHN reserves the right to deny a request for a list of accesses beyond the time period required by applicable law which is currently for a period of three (3) years prior to the date of the request; however, if the request is granted QHN may assess a reasonable, cost based fee.
Policy Dates	Written: February 10, 2016 Amended: July 28, 2020 Reviewed: July 28, 2020; July 12, 2023

	Section 10: Individual Opt Out Regarding HIE
Policy 10.0	**STANDARD**
	Individual Opt Out Regarding HIE: Individuals may request to Opt Out of HIE system query functionality. Opt Out does not prevent medical providers from directly exchanging Records within the HIE.
	POLICY
Individual notifies Participant	1) The Participant will be responsible for managing and responding to an Individual's request to Opt Out of HIE system query functionality. Should QHN receive a request from an Individual to Opt Out, QHN shall forward such request to the applicable Participant within five (5) business days.
Participant Reviews Requests and Implements Opt Out Restrictions	2) If an Individual has Opted Out: (a) Participants will NOT be able to access PHI about the Individual located in the HIE summary view, which includes PHI from Covered Entity Participants (sometimes referred to as the longitudinal health record), even in the case of an emergency; and (b) the Individual's treating medical providers may continue to use the HIE to exchange PHI, including diagnostic testing, results such as, lab and radiology results, medication history and insurance eligibility. 3) Participant is required to grant the Opt Out request to block future access to the Individual's summary view or longitudinal record.
QHN's Role	4) Opt Out shall be managed consistent with QHN Standards. QHN may provide information, assistance, and Opt Out forms to Participants as reasonably needed so that a Participant can manage the request, and counsel the Individual about the impact of Opting Out. 5) At its discretion, QHN may offer other methods for Individuals to Opt Out.
Policy Dates	Written: February 10, 2016 Amended: July 28, 2020 Reviewed: July 28, 2020; July 12, 2023

	Section 11: CRN Consent, Revocation and Care Teams
Policy 11.0	**STANDARD**
	CRN Consent: Except as set forth in this Policy, for an Individual's Records in the CRN System to be Used or Disclosed the Individual must authorize such Use and Disclosure by providing consent ("CRN Consent") meeting HIPAA Authorization requirements.
	POLICY
Only One Consent Required	1) An Individual's CRN Consent will be obtained before a Participant Uses or Discloses Records through CRN. A CRN Consent is not required when: a) Providing the minimum necessary Records to make a direct referral for services to another Participant, provided that other applicable legal requirements have been met. b) Records will be used by a Participant which directly obtained such Records from the Individual.
Consent Format	
Record of Consent Maintained for Six Years	2) Participants must use a CRN Consent that meets HIPAA Authorization requirements and is approved by QHN. CRN Consent may be obtained from the Individual in multiple formats allowed by law, such as written, verbal and electronic.
Participant to Document Consent	3) Participants must document and maintain completed CRN Consents as required by QHN and applicable law. CRN Consent must be maintained for a period of six (6) years after the date the consent has expired, or as required by applicable law. 4) CRN Consent may be documented by maintaining the consent in hard copy or electronic form, audio/video recording, an e-signature obtained by email, text message, or as allowed by applicable law. CRN Consent may be stored in the CRN system

Consent Expires After Two Years	based on then current functionality. If a completed CRN Consent is not stored in the CRN System, it must be maintained within the Participant organization acting as a custodian of QHN. QHN may require Participants to attest and verify that CRN Consent has been obtained as required by this Policy, and provide copies of Consents to QHN upon request. 5) A CRN Consent is effective for two (2) years from the date it is provided, unless revoked or a new CRN Consent is obtained.
Policy Dates	Written: July 28, 2020 Amended: _____ Reviewed: July 28, 2020; July 12, 2023

Policy 11.1	STANDARD
	CRN Consent Revocation: After providing CRN Consent, Individuals may revoke their consent.
	POLICY
Individual May Revoke Consent	1) The Individual may revoke CRN Consent by notifying a Participant that provides services to them. Authentication of the request may be required by the Participant or QHN before the revocation becomes effective.
Individual May Limit Consent	2) Within five (5) business days, after the revocation has been received and authenticated, the Participant or QHN will restrict access to Records, as required by the revocation. Participant shall promptly notify QHN of the revocation. Participant's actions within the CRN System restricting access to Records, shall be deemed a notification to QHN.
Use of Records Following Revocation	3) The revocation may be documented by maintaining the revocation in hard copy or electronic form, audio/video recording an e-signature or text message, as allowed by applicable law. The revocation may be stored in the CRN system based upon the then current system functionality and/or workflows. If a completed revocation is not stored in the CRN System, it must be maintained within the Participant organization acting as a custodian of QHN. QHN may require Participants or Participant Users to attest and verify that revocation has been obtained as required by this Policy, and provide copies of revocations to QHN upon request. 4) As allowed by applicable law, Records included in CRN prior to the revocation may continue to be Used and Disclosed by those Participants who had access to the Records prior to the revocation.
Policy Dates	Written: July 28, 2020 Amended: _____ Reviewed: July 28, 2020; July 12, 2023

Policy 11.2	STANDARD
	CRN Care Team Membership and Information Sharing: Care Teams ("Care Teams") may share information for the purpose of Care Coordination for an Individual through use of CRN.
	POLICY
Consent Required to Join Care Team Care Team Membership Individual may Restrict Access	1) Care Teams may only be formed for an Individual after CRN Consent has been obtained from that Individual. Participants serving an Individual <u>without</u> CRN Consent will only have access to the data provided to them per their engagement with the Individual. 2) Membership to the Care Team can be controlled in several ways at the option of the Individual: a) Individuals may approve every new request for a Participant to join the Care Team; b) Participants on their Care Team may approve requests to join the Care Team; and c) A Participant that wants to join their Care Team may add themselves at any point. 3) Prior to a CRN Consent being obtained from an Individual, a Participant may only use CRN: (a) to access information added to CRN about the Individual by the Participant, (b) to access limited demographic information, and (c) to make referrals for services for the Individual when permitted by applicable law. 4) After a CRN Consent has been obtained, Participants on an Individual's Care Team may have access to Records in CRN submitted by other Participants. 5) Individuals that have provided CRN Consent may have the ability to restrict specified Participant(s) who are on a Care Team from having access to their Records provided by other Participants. The CRN System may include additional functionality to accommodate Individual preference related to limiting the ability of Participants and Individuals to add Participants to the Care Team.
	6) As allowed by HIPAA, Records included in CRN prior to the restriction (removal from a Care Team) of a particular Participant's access may continue to be Used and Disclosed by the Participant who had access to the Records prior to the restriction.

Policy Dates	Written: Amended: Reviewed	July 28, 2020 July 28, 2020; July 12, 2023

	Section 12: Audit Rights
Policy 12.0	**STANDARD**
	Participant Right to Audit QHN Compliance: With regard to use and access to the QHN System, each Participant shall have a right to audit: QHN's compliance with the terms of the Electronic Commerce Agreements it has with QHN; access that has been made to Records placed in the QHN System by the Participant; and QHN's security and privacy Policies and procedures.
	POLICY
Notice to be Given	1) Any Participant wishing to conduct an audit of QHN as permitted by this Policy shall provide written notice to QHN at least two (2) weeks in advance. Such notice shall include specific information as to what records or other information that the Participant wishes to review during the course of the audit, and the number and identification of persons who will perform the audit. The notice shall also state suggested dates and times for the audit, and an estimate of how long the audit will last.
Access to Records for Audit Purposes	2) The audits will be scheduled by mutual agreement between QHN and Participant. No more than one audit by Participant may be conducted during any calendar year, unless the audit is prompted by an identifiable threat to the security or privacy of Records or is required by applicable law. 3) When appropriate notice has been provided to QHN of a Participant's intent to perform an audit, QHN will provide access to the records or other information specified in the notice on the mutually agreed upon date and time. A reasonable workspace for the auditors will also be provided by QHN if an onsite audit is being conducted.
Confidentiality Agreements	4) Each auditor acting on Participant's behalf shall sign a confidentiality agreement (in addition to any other confidentiality agreements already in place) in a form acceptable to QHN prior to performing the audit.
Hours of Audit	5) Auditors acting on Participant's behalf shall only be permitted to have reasonable access to QHN records and information during the normal business hours of QHN.

Expenses Incurred	6) Any expenses incurred by QHN as a result of a Participant audit shall be the responsibility of the Participant. QHN may require prepayment of estimated expenses.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 12.1	STANDARD
	QHN Right to Audit Participant Compliance: QHN shall have a right to audit each Participant's compliance with the terms of any agreement Participant has with QHN, Participant's and Participant User's compliance with QHN Standards and related procedures, and security and privacy policies that a Participant has in place with regard to use of and access to the QHN System.
	POLICY
Notice to be Given Access to Records for Audit Purposes Hours of Audit Expenses Incurred	1) QHN shall provide a Participant written notice at least two (2) weeks in advance. Such notice shall include specific information as to what records or other information that QHN wishes to review during the course of the audit, and the number and identification of persons to perform the audit. The notice shall also state suggested dates and times for the audit, and an estimate of how long the audit will last. 2) The audits will be scheduled by mutual agreement between QHN and Participant. No more than one audit by QHN of a particular Participant may be conducted during any calendar year, unless the audit is prompted by an identifiable threat to the security or privacy of Records or is required by applicable law. 3) When appropriate notice has been provided to Participant of QHN's intent to perform an audit, Participant will provide access to the records or other information specified in the notice on the mutually agreed upon date and time. A reasonable workspace for the auditors will also be provided by Participant if an onsite audit has been agreed to. 4) Auditors designated by QHN shall only be permitted to have reasonable access to Participant records and information during the normal business hours of Participant. 5) Any expenses incurred by Participant as a result of a QHN audit shall be the responsibility of QHN. The Participant may require prepayment of estimated expenses.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 12.2	STANDARD
	System Use: Audits/Audit Controls: Participants are responsible for auditing Participant Users' use of, and access to, the QHN System to ensure such use and access is appropriate.
	POLICY
System Activity Recorded	1) QHN will record System activity and access through hardware and software mechanisms that record System activity and access to Records.
Participant to Review	2) QHN can generate reports that show Individual Records accessed by Participant Users ("Report"). The content and format of the Reports will be as determined by QHN. Upon request by a Participant, QHN may generate and provide more detailed Reports to be given to the Participant for their review. Participants are ultimately responsible for ensuring use of and access to the QHN System by their Participant Users is appropriate. Participants are required to notify QHN's Privacy and Security Officer about any suspected unauthorized accesses to patient information.
Summary Level Report Available	3) A summary level Report may be distributed to Participants periodically. Participants are required to review the Reports. Upon request, more detailed reports may be made available to assist them in audits of Participant User activity. Additional expenses to create more detailed reports shall be the responsibility of Participant, and QHN may require prepayment of estimated expenses.
	4) At its discretion, QHN may generate and distribute to Participants, reports of other applications and access to or within the QHN System.
	5) The QHN Privacy and Security Officer will follow up on any reported unauthorized access. All findings will be reported to the QHN Executive Director with further review, audit or other subsequent action to be taken, as deemed appropriate by the Executive Director.

User Sanctions	6) If QHN becomes aware of Participant User's misuse of the QHN System, the Participant User and the respective Participant may be subject to sanctions as set forth in these QHN Policies and the Participant's Electronic Commerce Agreement, up to and including termination of rights to access and Use the QHN System.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 12.3	STANDARD
	Immediate Audit by QHN: QHN has the right to perform an immediate audit of any Participants' Use of the QHN System should the QHN Executive Director determine that facts and circumstances warrant an immediate audit is necessary.
	POLICY
QHN's Right to Perform an Immediate Audit QHN Retains Sole Discretion	1) Should facts and circumstances warrant, QHN has a right to perform an immediate audit of Participant's records related to Use of the QHN System. 2) QHN will provide Participant with as much notice as reasonably possible in the event QHN elects to perform an immediate audit. 3) QHN will provide Participant with reasons for the immediate audit at the time notice is provided. However, the decision to perform the immediate audit remains solely at the discretion of QHN. 4) Upon notice to Participant by QHN, Participant shall provide QHN access and cooperation so that QHN may conduct an audit as described above.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 12.4	STANDARD
	Audits by Government and Other Organizations: QHN shall permit audits of QHN's records to the extent required by law or agreements to which QHN is a party.
	POLICY
Access Allowed	1) QHN shall allow access to the QHN System and records for audit purposes to a governmental agency or other organization with which QHN has an agreement, to the extent required by law or agreements to which QHN is a party.
Record of Audits	2) QHN's Privacy and Security Officer shall keep a detailed record of these audits. The records shall include names of agencies, dates of audits and reasons for the audits. If an audit results in the provision of access to PHI, then the access shall be logged pursuant to applicable law and regulation.
Audit Findings Retained	3) Any audit findings provided to QHN shall be retained by QHN per QHN's record retention policies 4) Audit findings will be made available to QHN Participants, at QHN's discretion.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

	Section 13: Subpoenas/Law Enforcement Inquiries
Policy 13.0	**STANDARD**
	Subpoena for Records: QHN shall respond to subpoenas for Records promptly and in accordance with HIPAA and all other applicable federal and state law.
	POLICY
Role of Privacy and Security Officer Subpoenas are Logged Fees May be Assessed	1) Subpoenas for Records received by QHN shall be directed to the Privacy and Security Officer or their designee and acted upon appropriately. 2) QHN shall keep a log of any subpoenas for Records received by QHN, and shall maintain information about the subpoena and response by QHN as may be required by HIPAA and other applicable law. 3) QHN may charge a reasonable fee associated with handling and responding to subpoena.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 13.1	STANDARD
	Law Enforcement Inquiries for Records: QHN shall respond to law enforcement inquiries for Records promptly and in accordance with HIPAA and all other applicable laws.
	POLICY
Role of Privacy and Security Officer Inquiries are Logged Fees May be Assessed	1) Any law enforcement inquiry for Records received by QHN shall be directed immediately to the Privacy and Security Officer or their designee and acted upon appropriately. 2) QHN shall keep a log of any law enforcement inquiries for Records received by QHN and shall maintain information about the inquiry and response as may be required by HIPAA and other applicable law. 3) QHN may charge a reasonable fee associated with handling and responding to law enforcement inquiries.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016; July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

	Section 14: Research
Policy 14.0	**STANDARD**
	Research Request Procedures: QHN may allow for and consider data requests for research purposes. Research requests require approval by three fourths (3/4) of the members of the Board of Directors as described below. For purposes of this policy, the term "research" is defined as provided in HIPAA to mean: a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
	POLICY
Requests Reviewed by Executive Director Content of Request	1) All requests of Records and data for research purposes shall be made in writing by the requesting organization, and be reviewed by the Executive Director or designee. If required by the Executive Director, the request shall include information such as that contained on the QHN Research Request Form, a sample of which can be found in the "Supplemental Information" section at the end of these QHN Policies. The Executive Director may require any other information reasonably required to complete an informed review of such request. This may include, for example, the following types of information: A. a description of the issue to be researched and supporting documentation; B. a list of the data points needed to perform the research; C. a list of the principal Participants, organizations and their roles, indicating the primary contact person and their contact information; D. a description of the expected results from the research; E. a list of the potential positive and or negative impacts of the research; F. the budget for or associated with the research and source(s) of funding to conduct the research; G. the time frame for the project; and H. Confirmation that the request and proposed Use of the data complies with applicable law.

Actions taken in response to request	2) The Executive Director may take one of the following actions with respect to a research request: A. Deny the research request; or B. Submit the request to the Board of Directors for final review with a recommendation regarding the request. In making a recommendation, the Executive Director may request review and input from a review committee or subject matter experts.
BOD Approval	3) Approval by three fourths (3/4) of the members of the Board of Directors is required for approval of any research request submitted. If the request is approved at a Board of Directors meeting by all Directors present at the meeting, approval by the absent Directors may be obtained electronically from any board member not present at the meeting wherein the research request was reviewed.
	4) With respect to any research request decisions by the Board of Directors any denial or approval must be recorded in the minutes of the meeting along with an explanation of the reason for the decision(s).The Executive Director or his/her designee will notify the requesting organization of QHN's decision regarding the request.
Request to Comply with Applicable Law	5) No request will be approved unless the proposed recipient of data specifies and agrees that data will only be used in accordance with applicable law.
Research by QHN	6) When QHN or a subcontractor acting on QHN's behalf is conducting research, QHN or the subcontractor will comply with applicable law and the terms of applicable E-Commerce Agreements. Approval by the Board of Directors, as required in this policy, is not required for QHN or QHN subcontractors conducting research.
Policy Dates	Written: August 25, 2005 Amended: January 15, 2014; February 10, 2016, July 28, 2020 Reviewed: December 21, 2011; January 15, 2014; February 10, 2016; July 28, 2020; July 12, 2023

Policy 14.1	STANDARD
	Data Must be De-identified: QHN will not allow release of data that is not De-identified or in a limited Data Set to be used for research purposes, except under certain circumstances.
	POLICY
Data De-identified or Limited Data Set De-identified Data Exceptions	1 Board of Directors' approved data research projects under Policy 14.0 will be delegated to the Executive Director for assignment to QHN employee(s) (or subcontractor) who will retrieve the data. 2) Except as provided in paragraph 4 below, all data provided to the requesting entity for research projects will (a) Be de-identified as provided for in HIPAA or will meet HIPAA requirements for limited data set disclosures (i.e. 45 C.F.R. 164.514(e)) if the information includes PHI, and (b) Have all individual identifiers removed as may be appropriate and required by applicable law if the information includes only CSI. 3) Disclosure of a limited data set may only occur pursuant to a HIPAA compliant "Data Use Agreement" approved by the Executive Director. 4) As an exception to the requirement of 2(a) above to provide only De-Identified data or a "limited data set", Records may be disclosed if the following requirements are met: A. Such Use and Disclosure is approved by the QHN Board of Directors as provided for in Policy 14.0, and B. Such Use and Disclosure is in compliance with applicable law, including appropriate Institutional Review Board review.
Policy Dates	Written: August 25, 2005 Amended: January 15, 2014; February 10, 2016; July 28, 2020 Reviewed: December 21, 2011, January 15, 2014; February 10, 2016; July 28, 2020; July 12, 2023

	Section 15: HIPAA Compliance
Policy 15.0	**STANDARD**
	Privacy/Security Officer: QHN shall establish and maintain appropriate administrative, physical and technical safeguards, in accordance with the HIPAA Security and Privacy Rule, other applicable law, and agreements to which QHN is party in order to appropriately protect PHI. QHN shall designate a person who shall have the responsibility to ensure that appropriate policies and procedures are developed, implemented and maintained
	POLICY
QHN designates QHN Privacy/Security Officer(s)	1) QHN will identify a person or persons as the QHN Privacy/Security Officer(s) who is/are responsible for the development and implementation of HIPAA privacy/security Policies and procedures. Such policies and procedures shall be designed to: A. Ensure the confidentiality, integrity, and availability of all PHI that QHN creates, receives, maintains, or transmits. B. Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI. C. Protect against any reasonably anticipated Uses or disclosures of PHI that are not permitted or required under HIPAA, other applicable law, and agreements to which QHN is a party. D. Ensure compliance with HIPAA by QHN's workforce.
Roles of QHN Privacy/Security Officer(s)	2) The QHN Privacy/Security Officer(s) shall employ reasonable methods to assure that use of the QHN System by QHN employees is in compliance with HIPAA, all other applicable law, and agreements (including but not limited to Business Associate Agreements) to which QHN is a party. Use of the

	system by QHN employees includes any Use or Disclosure of PHI. 3) The QHN Privacy/Security Officer(s) is/are responsible for taking reasonable actions to help ensure that use of the QHN System by all Users is in compliance with HIPAA and all other applicable law. 4) The QHN Privacy/Security Officer(s) shall ensure that QHN has policies and procedures in place that require disposal of PHI be in compliance with all applicable law. 5) The QHN Privacy/Security Officer(s) shall ensure reasonable measures are established to protect the QHN facilities from unwanted intrusions. 6) The QHN Privacy/Security Officer(s) shall work with the QHN staff responsible for implementing QHN System access by Participant Users, proper User identification methods and other security safeguards to assure secure access by QHN Users. 7) The QHN Privacy/Security Officer(s), in conjunction with the appropriate QHN committee, Executive Director, QHN support staff, and external consultants as deemed appropriate, shall identify, address and respond to any other security and privacy incidents, issues, or complaints which may arise.
Policy Dates	Written: August 25, 2005 Amended: April 17, 2013; February 10, 2016; July 28, 2020 Reviewed: December 21, 2011, April 17, 2013; February 10, 2016; July 28, 2020; July 12, 2023

Policy 15.1	STANDARD
	Disaster Recovery/Data Backup/Contingency Plans: QHN shall maintain plans for disaster recovery, data backup, contingency operations and other related plans, in compliance with the HIPAA Security Rule and applicable laws.
	POLICY
Disaster Recovery Plans in Place	1) QHN shall create a Disaster Recovery Plan to restore any loss of data and Records, Data Backup Plan to create and maintain retrievable copies of electronic Records and all other Contingency Plans to continue critical business activities in the event of a disaster. These plans shall provide for the resumption of QHN operations within a reasonable time following a disaster or data loss.
Plans Reviewed Periodically	2) QHN shall periodically review and test the Disaster Recovery Plan, Data Backup Plan and Contingency Plan. Such plans will also be reviewed in response to material changes to the QHN System or changes effecting the security of Records maintained by QHN. 3) To support decision making regarding QHN's Disaster Recovery Plan, Data Backup Plan and Contingency Plans, QHN shall perform and appropriately update any applications and Data Criticality Analysis.
QHN Vendors and Subcontractors	4) QHN will require its contractors, vendors, subcontractors, or other service providers that store or host Records for use as part of the QHN System to have or cooperate in the establishment of Disaster Recovery Plans, Data Backup Plans and Contingency Plans as necessary to comply with this Policy.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016; July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 15.2	STANDARD
	Facility Access and Security Controls: Access to the QHN facility, located on QHN's premises, or in other locations, is secured in compliance with HIPAA and other applicable law.
	POLICY
Visitors Accompanied	1) All visitors at a QHN facility shall register upon entry or shall be accompanied by a QHN staff member during the visit.
QHN Facilities Secured	2) All facilities under QHN's control and any vendor facility at which PHI or electronic PHI can be accessed or which houses equipment that controls access to PHI or stores electronic PHI, on behalf of QHN, shall be locked and secured outside of normal business hours.
Maintenance Records	3) Any rooms or offices where QHN System hardware, computer servers, or other equipment is located shall be locked and secured at all times and access shall be appropriately restricted to authorized persons whose job functions necessitate access. Access to such data rooms or offices by persons, including vendors, who do not have regular authorized access rights shall be logged.
	4) Appropriate maintenance records will be kept of material repairs or modifications related to the physical security components of the facility (e.g. locks, keys, hardware, walls, and doors).
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 15.3	STANDARD
	Workstation Security/Encryption: QHN employees shall follow QHN's workstation security procedures to minimize unauthorized access to Records or other confidential information and to limit risk to QHN's information networks and the QHN System.
	POLICY
Workstations Encrypted at Rest	1) Employee workstations (including desktop and laptop computers or other computer devices) shall be secured in accordance with QHN security procedures. All servers or other computer devices containing or storing electronic PHI shall be encrypted at rest in accordance with HIPAA and applicable regulatory guidance. Employees are strongly discouraged from storing PHI on their desktop or laptop computers.
No PHI on Mobile Phones	2) Employees shall not store any Records, even if it is encrypted, on any smart phone, or similar device.
	3) QHN employees and contractors shall take appropriate measures to protect the privacy of Records in any work area.
Portable Devices Secured	4) Portable devices used by QHN employees or contractors shall be protected by appropriate security controls and technology, as determined by QHN and in accordance with applicable security regulations and other specific Procedures adopted by QHN.
No Records on Removable Media	5) Unless approved by the Executive Director or his designee, no Records, regardless of whether it is encrypted, will be stored locally on any removable media, including, but not limited to: floppy disks, portable disk drives, or USB Flash Memory drives.
Confidentiality Agreement Required for Third Party Access	6) QHN shall ensure that third parties are not given access to or use of QHN office equipment containing Records or other confidential information, unless an appropriate written confidentiality agreement is in place.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 15.4	STANDARD
	Use of Technology/Workstation Use: Every QHN employee shall follow QHN procedures for use of technology to minimize unauthorized access to Records or other confidential information and to limit risk to QHN's information networks and the QHN System.
	POLICY
	1) For details as to QHN's procedures regarding use of technology by QHN employees, refer to the QHN Employee Handbook, which is incorporated here by this reference. 2) As further detailed in the QHN Employee Handbook, workstation use, including laptop use, is generally restricted to appropriate job related activity, except as permitted or required by applicable laws.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 15.5	STANDARD
	Transmission of PHI is Secured: Transmission of PHI under the control of QHN is secured in accordance with HIPAA and other applicable laws.
	POLICY
QHN Transmission of PHI Secured	1) Transmission of PHI under the control of QHN is secured in accordance with HIPAA and generally accepted security standards.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016; July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 15.6	STANDARD
	Equipment Repair/Disposal/Tracking: QHN Equipment containing Records, or other sensitive information will be tracked, repaired and disposed of in compliance with HIPAA and all other applicable laws.
	POLICY
Service / Repair Complies with HIPAA	1) Service or repair of QHN equipment containing Records or other sensitive data will be conducted in accordance with HIPAA security requirements, including, but not limited to, removal of all Records prior to shipping. Additional related requirements and detail are provided in the QHN Employee Handbook, which is incorporated here by reference.
QHN Hardware Containing PHI Controlled	2) QHN shall log and track any and all computer hardware, servers, or other computing equipment or devices which store or are used to maintain electronic Records. The QHN Privacy/Security Officer or the Officer's designee is responsible for maintaining logs and records regarding the location of such equipment or devices and any movement or relocation shall be documented, regardless of whether such equipment or devices are under the direct control of QHN or under the direct control of a contractor, vendor, subcontractor, or other service provider.
Destruction of Hardware Complies with HIPAA	3) Any computer hardware or computing equipment containing or storing Records shall be appropriately destroyed and electronic PHI must be completely removed when such equipment is no longer used or is disposed of.
QHN Vendors and Subcontractors To Comply	4) QHN will require its contractors, vendors, subcontractors, or other service providers that maintain Records to cooperate with QHN for purposed of complying with this Policy.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016; July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 15.7	STANDARD
	QHN System Security Evaluation, Audits and Risk Analysis: QHN shall conduct, or cause to be conducted security evaluations, audits and risk analysis (collectively "Reviews") of the QHN System. The security Reviews will be conducted in compliance with the requirements of HIPAA.
	POLICY
Scope of Security Reviews Reviews Conducted Periodically	1) QHN's security management process shall require implementation of Procedures designed to prevent, detect, contain, and correct security incidents and violations, and to assess and reduce potential risks and vulnerabilities to the confidentiality, availability and integrity of PHI. 2) Reviews required by this Policy shall be conducted periodically, in response to material operational or environmental changes, or as directed by the QHN Executive Director, and shall include the following: A. Evaluation of the likelihood and impact of potential security risks to PHI. B. Developing plans to implement or modify security measures to reasonably and appropriately address and reduce the risks identified in the Review; and C. Documenting the Review and chosen security measures and, where required, the rationale for adopting those measures.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed February 10, 2016; July 28, 2020; July 12, 2023

	Section 16: Employee Clearance/Training
Policy 16.0	**STANDARD**
	Background Checks Required: QHN shall conduct a background check for all employees hired by QHN. Employee access to the QHN System, Records, and other confidential information will be determined and limited in accordance with job duties and roles.
	POLICY
Background Checks Required for QHN Employee	1) Prospective employees are required to submit to QHN a completed Application for Employment and all other documents required by QHN. The background check must be completed prior to beginning employment. QHN may also conduct background checks regarding current employees.
Authentication Requirements and Role-Based Access	2) The employee's job function will determine the role-based access they will be granted to the QHN System, Records, or other confidential data. Employees are provided the appropriate "minimum necessary" access for their job functions. Access is reviewed by the QHN Privacy/Security Officer(s).
Changes to Access	3) Changes to system access for QHN employees will be reviewed by the QHN Privacy/Security Officer.
Policy Dates	Written: August 25, 2005 Amended: December 21, 2011; February 10, 2016 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 16.1	STANDARD
	Employee Training: QHN shall provide HIPAA privacy and security training and ongoing awareness training for all its employees.
	POLICY
HIPAA Privacy and Security Training Proof of HIPAA Training Ongoing Awareness Training	1) QHN shall provide HIPAA privacy and security training for all its employees. Such training shall include, but not be limited to, familiarity with HIPAA privacy and security laws as they relate to each employee's job duties. Training may also address and include privacy and security requirements to be followed regarding Records as may be appropriate when considering requirements of E-Commerce Agreements and applicable law. 2) QHN shall maintain documentation of each employee's HIPAA training. 3) QHN shall regularly provide employees with security reminders and periodic security updates, and raise awareness regarding security threats, including information related to protection from malicious software and appropriate procedures for guarding against, detecting, and reporting malicious software.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016; July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

Policy 16.2	STANDARD
	Administrative Access of QHN System: QHN has in place procedures that allow secure administrative access of the QHN System.
	POLICY
Administrative Accounts Secure	1) For approved QHN employees, contractors or vendors, individual administrative accounts are created that allow secure administration and maintenance of the QHN System. 2) Each administrative account is specifically identifiable to the particular employee, contractor or vendor. 3) Accounts are disabled when administrative access is no longer required.
Administrative Accounts Reviewed	4) The QHN Privacy/Security Officer(s) periodically review(s) and audits administrative account access so as to ensure appropriate system use that is compliant with HIPAA and other QHN Standards
Administrative Logins Secure	5) QHN administrative account login credentials shall be robust and strong and meet appropriate levels of security, as determined by the QHN Privacy/Security Officer.
Policy Dates	Written: December 11, 2007 Amended: _____ Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

	Section 17: Sanctions
Policy 17.0	**STANDARD**
	Sanctions for Non-Compliance: Failure or alleged failure of a Participant or Participant User to comply with either the QHN Policies or terms of any written agreement between Participant and QHN shall result in an investigation and possible sanctions.
	POLICY
Discovery by QHN and Notice to Participant	1) Where QHN discovers or becomes aware of noncompliance with QHN Policies or terms of a written agreement between Participant and QHN by a Participant or Participant User, the QHN Executive Director or Privacy/Security Officer shall notify the Participant of the issue in writing.
Temporary Restrictions	2) QHN reserves the right to restrict access to the QHN System at the time of discovery, pending further investigation.
Responses in Writing	3) Participant shall respond in writing to the notice within five (5) business days with a full description of the circumstances surrounding the failure or alleged failure to comply.
Executive Director Determines Sanctions	4) If the Executive Director, after reviewing the matter, determines that the Participant or Participant User failed to comply with the QHN Policies or terms of a written agreement with QHN, the Executive Director shall determine the type of sanction(s), if any, to be imposed. 5) The Executive Director has discretion as to the sanction(s) to be imposed. The Executive Director may consult with the Board of Directors or appropriate QHN committee(s) before deciding on a sanction(s).
Report to Licensing Authority Possible	6) Sanctions may include, but not be limited to, the following: an admonishment, suspension or termination of rights to use the QHN System, limiting the rights to use the QHN System, imposing certain requirements for or prohibiting future use of the QHN System. QHN may also notify the appropriate licensure board or other organizations with whom a Participant or Participant User has a relationship or privileges. 7) QHN shall provide notice of a sanction to the Participant and Participant User.

Right to Appeal	8)	Participants or Participant Users may request an appeal to review the sanctions. Written appeal for review of sanctions must be received by QHN within five (5) business days of notification of the sanction.
Role of the Board	9)	The Board of Directors, or a sub-committee of Board members appointed by the Board to act on its behalf, shall review the written appeal of the sanction(s). The Participant and Participant User have the right to appear at the Board meeting or sub-committee meeting to present the Participant and Participant User's position regarding the appeal. The manner and conduct of the meeting shall be at the sole discretion of the Board of Directors or sub-committee. The Board of Directors or sub-committee decision on the appeal shall be final.
Right to Immediate Sanction by Executive Director	10)	Notwithstanding the other terms of this policy, the Executive Director shall have the right to immediately suspend or otherwise limit a User's access to the QHN System if the Executive Director, at the Executive Director's sole discretion, determines that such suspension or limitation prior to an investigation is necessary to avoid the potential of continuing violations of applicable law or to avoid harm or damages to the QHN System, QHN, Participant(s), Participant User(s), or to an Individual whose Records are in the QHN System. In such a circumstance, the Executive Director will conduct an investigation as soon as reasonably possible.
Circumstances when Sanction Policy does not Apply	11)	This sanction policy is not applicable when (a) QHN is exercising its rights under an Electronic Commerce Agreement or other agreement with a Participant or Participant User, or (b) the person is no longer a Participant User (for example, is no longer an employee of the Participant).
Policy Dates	Written:	August 25, 2005
	Amended:	December 10, 2008; December 21, 2011; February 10, 2016; July 28, 2020
	Reviewed:	December 10, 2008; December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 17.1	STANDARD
	Employee and Subcontractor Sanctions: Failure or alleged failure of a QHN employee or QHN subcontractor to comply with QHN Standards, applicable law, or any written or oral agreement between the employee and QHN will result in an investigation and possible sanctions.
	POLICY
Disciplinary Actions	1) Failure to comply with QHN Standards, applicable law, or any written or oral agreement between an employee or a subcontractor and QHN may result in disciplinary action up to and including termination of employment or termination of the subcontractor's agreement with QHN. Such employee or subcontractor shall be liable for all damages sustained by QHN, including attorney fees. 2) Nothing in this Policy shall be construed to alter or change the "at will" employment status of any employee.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016; July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

	Section 18: Confidentiality Agreements
Policy 18.0	**STANDARD**
	QHN Employee Confidentiality: All QHN employees shall enter into confidentiality agreements with QHN, as required by QHN.
	POLICY
	1) In addition to the particular terms and conditions of the QHN employee confidentiality agreement the QHN Employee Handbook may also include additional confidentiality requirements
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 18.1	STANDARD
	Participant Confidentiality: Participants are responsible for Participant Users' protection of confidential information.
	POLICY
Participant and Participant Users are Responsible for Confidentiality Confidentiality Obligations Continue After Termination of System Access.	1) Participants and Participant Users shall hold in confidence all Records placed in or accessed from the QHN System in accordance with applicable law. 2) Participants and Participant Users shall also hold in confidence all "QHN Confidential Information," which includes: business, information, trade secret, design, process, procedure, formula, intellectual property information, software, computer code, and any data or information that is not generally known by the public, such as policies and procedures, document forms, business processes, marketing strategies, pricing policies, financial information, referral sources, customer or patient lists, subcontractor, vendor, or supplier information, provider information, accounts payable and receivable, information concerning employees, physical plant and facility configuration and security, and internal performance results or security reviews. 3) Obligations to hold Records and QHN Confidential Information confidential shall continue after termination of the Participant User's access to the QHN System.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

	Section 19: DURSA Requirements
Policy 19.0	**DURSA STANDARD**
	DURSA Participants Response to Requests: DURSA Participants that seek message content for treatment through the eHealth Exchange have a duty to respond to messages that seek message content for treatment, as required by the DURSA.
	POLICY
	1) The QHN System will respond to messages that seek message content through the eHealth Exchange by providing a response to the query with the requested message content if it is appropriate to do so under terms of the DURSA and pursuant to QHN Policies, or respond with a standardized response that indicates message content is not available or cannot be exchanged. 2) All responses to messages will comply with the eHealth Exchange requirements under the DURSA. 3) Notwithstanding any other provision of these Policies, a participation agreement may be required by QHN for a person or entity seeking information from the QHN System. The DURSA shall not be considered such a participation agreement. If a participation agreement is not entered, then QHN will comply with applicable law in determining how and when to respond to requests for information through the DURSA.
Policy Dates	Written: August 17, 2011 Amended: July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 19.1	DURSA STANDARD
	DURSA Adverse Security Event and Breach Notification: QHN and DURSA Participants shall comply with the breach and "adverse security event" notification requirements under the DURSA
	POLICY
	1) Within one (1) hour of determining that an "adverse security event" (as defined by the DURSA) has occurred that involves a "federal participant" (as defined by the DURSA), QHN shall alert the federal participant in accordance with the procedures and contacts provided by such federal participant, and (b) within twenty-four (24) hours after determining that an adverse security event has occurred and is likely to have an adverse impact on a federal participant(s), QHN shall provide a notification to other DURSA Participants that are likely impacted by the event, and the Coordinating Committee, in accordance with the procedures and contacts provided by such federal participant. 2) As soon as reasonably practicable, but no later than five (5) business days after determining that a breach or an "adverse security event" (as defined in the DURSA) has occurred, the DURSA Participant shall notify QHN and will assist and cooperate with QHN in the notification by QHN of any other clinical messaging system likely impacted by the breach of unsecured PHI and the eHealth Exchange Coordinating Committee or its designee of the breach or "adverse security event" as required by the DURSA. Notification by a DURSA Participant to QHN shall include all information required by QHN standards and the DURSA including obligations to supplement information provided.
Policy Dates	Written: August 17, 2011 Amended: July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 19.2	DURSA STANDARD
	QHN and DURSA Participant Requirements: QHN and DURSA Participants shall comply with all other requirements of the DURSA.
	POLICY
	Each DURSA Participant shall: 1) Comply with all applicable law; 2) Reasonably cooperate with QHN on issues related to the DURSA; 3) Submit a message through the eHealth Exchange only for permitted purposes as defined under the DURSA; 4) Use message content received through the eHealth Exchange in accordance with terms and conditions of the DURSA; 5) As soon as reasonably practicable after determining that an adverse security event or breach of unsecured PHI has occurred, report such breach to QHN; and 6) Refrain from disclosing to any other person any passwords or other security measures issued to Participant or Participant User by QHN.
Policy Dates	Written: August 17, 2011 Amended: July 28, 2020 Reviewed: December 21, 2011; February 10, 2016; July 28, 2020; July 12, 2023

Policy 19.3	DURSA STANDARD
	DURSA Agreement with QHN: Prior to Using and accessing the QHN System for purposes of Transacting under the DURSA, each User shall have complied with all identification, credentialing, enrollment and access requirements of that User's respective DURSA Participant. Additionally, each such User shall comply with the Information Privacy and Protection Laws and all applicable policies of the respective DURSA Participant, including but not limited to policies regarding the Use of and access to message content.
	POLICY
Authentication Requirements Denial of Access to Message Content (DURSA Participants)	1) When QHN has not issued the identification credentials of the individual submitting message content (as defined in the DURSA), it is the responsibility of that individual's respective DURSA Participant to verify the identity of the submitter prior to the Transaction of message content. 2) If QHN has specific information which would cause QHN to question that identity or credentials of an individual credentialed by another DURSA Participant, or the security or integrity of another DURSA Participant, QHN shall cease to Transact all message content with that individual / DURSA Participant and provide notification to the Coordinating Committee as set forth in the DURSA.
Policy Dates	Written: December 21, 2011 Amended: July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

	Section 20: QHN Policy Compliance Review and Participant Notice
Policy 20.0	**STANDARD**
	QHN Policies Reviewed Periodically and Participants Notified: QHN shall periodically audit its compliance with the QHN Policies, as well as review the adequacy of these QHN Policies.
	POLICY
Policies Reviewed for Compliance Frequency Notice to Participants	1) The QHN Privacy/Security Officer is responsible for evaluating QHN Policies, to assure compliance with HIPAA and all other applicable laws. 2) The policy review shall be performed periodically and in response to material operational or environmental changes. 3) Notice will be given to Participants when any substantive revisions, additions or changes are made to these Policies that may impact the security or privacy of Records, or Participant or Participant User requirements or obligations under the Policies or related Procedures. Notice may be provided by any reasonable means, including by email to the Participant, with the goal of providing notice within thirty days of any revision, addition or change.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016; July 28, 2020 Reviewed: February 10, 2016; July 28, 2020; July 12, 2023

SUPPLEMENTAL INFORMATION

(See Policy 14)

1) Research Request Form:

Title of project: _____

Requesting organization: _____

A. Present the problem/issue to be researched.

B. A list of the data points needed to perform the research.

C. List the principal Participants, organizations and their roles, indicating the primary contact person including contact information.

D. Describe the expected results from the research.

E. List the potential positive and or negative impacts of the research.

F. Present the budget attached to the research.

G. Describe the time frame for the project.

By signing below, I confirm and acknowledge:

(1) that this request and proposed Use of the data complies with applicable law;
(2) that the information provided above (or attached) is true and correct;
(3) that I may be required to provide additional information in support of this request, and that any additional information I provide will be true and correct.

_____ _____

Signature Date

_____

Printed name /title

SUPPLEMENTAL INFORMATION

(See Policy 1.6)

SAMPLE LANGUAGE: Participant Notice to Individuals about HIE Participation:

Our organization uses the Quality Health Network ("QHN") health information exchange system ("HIE") for the secure exchange of electronic health information between authorized medical providers. The HIE protects patient privacy by using various security features that include encryption, password protection and information access and audit controls.

In some cases, you may limit a medical providers' ability to view your health information through use of the HIE. This right is referred to as "Opt-Out".

If you choose to Opt-Out a medical provider who you are seeing for care, will NOT be able to view your health information via an HIE query, EVEN IN AN EMERGENCY. Opting Out can inhibit access to critical information that may help your medical providers manage your care and may increase duplication and costs.

However, your medical provider(s) may continue to use the HIE to electronically direct the exchange of your health information, such as diagnostic test results.

To Opt-Out, you must complete a written request with your medical provider. If you want more information about the HIE or to discuss Opt-Out, please contact your medical provider.