QUALITY HEALTH NETWORK

Health Information Exchange Governing Policies

Amended
February 10, 2016

Dick Thompson
Executive Director and CEO
dthompson@qualityhealthnetwork.org
Justin Aubert
Chief Financial Officer
jaubert@qualityhealthnetwork.org
Marc Lassaux
Chief Technical Officer
mlassaux@qualityhealthnetwork.org
Janet Terry
Privacy and Security Officer
jterry@qualityhealthnetwork.org

744 Horizon Court, Ste 210
Grand Junction, CO 81506
Phone: 970-248-0033
Fax: 970-248-0043

TABLE OF CONTENTS

These policies contain amendments to the QHN Policies that were in effect as of February 9, 2016. The policies are effective February 10, 2016.

INTRODUCTION AND DOCUMENTS INCORPORATED BY REFERENCE

The following Policies of Quality Health Network 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 are incorporated and made part of the "QHN Standards" which are referenced in the Electronic Commerce Agreements between QHN and Participants. These Policies are adopted by the Board of Directors and are subject to revision, modification or change by the Board of Directors. Through the Electronic Commerce Agreements and Use of the QHN System, 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 policies. Participants are encouraged to provide input regarding these Policies and to propose changes.

Many of these Policies are supported by underlying detailed Procedures, which are incorporated by reference. Copies of all QHN Standards, and the more detailed Procedures which are incorporated by reference as part of these Policies (and therefore also are part of the QHN Standards), may be reviewed upon request.

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. All terms defined in the QHN Policies shall have a meaning consistent with terms defined in HIPAA. Capitalized terms in the QHN Policies are defined as follows:

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

2) "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.

3) "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.

4) "Directed Exchange" shall mean the transmission and receipt (*i.e.*, exchange) of Medical Records and other information between or among specific Participants where each such Participant has a relationship with the Individual about whom the information pertains. For example, a physician may receive lab results using Direct Exchange services provided by the QHN System.

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

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

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

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

9) "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.

10) "Individual" means a natural person who is the subject of PHI.

11) "Information Privacy and Protection Laws" mean (i) HIPAA; (ii) the Health Information Technology for Economic and Clinical Health Act in the American Recovery and Reinvestment Act of 2009, including any implementing regulations ("HITECH"); (iii) the Gramm-Leach-Bliley Act, as amended and including any implementing regulations; (iv) any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy or security of information pertaining to the health or medical status or condition of an Individual, and/or the payment for health or medical care for an Individual; (v) any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy of information pertaining to the financial or credit status or condition of an Individual; (vi) any statute, regulation, administrative or judicial ruling requiring a party to protect information pertaining to Individuals based upon the Individuals' status as consumers; and (vii) 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 and Protection Laws have been enacted, promulgated, issued or published by any federal or state governmental authority with jurisdiction over an Individual, a Participant or QHN.

12) "Licensed Health Care Provider" shall mean an Individual who is licensed to provide health care services and whose license is currently active and in good standing.

13) "Medical Records" shall mean any documents containing information related to an Individual for whom medical care is provided.

14) "Opt Out" shall mean that access to an Individual's Medical Records located in the Patient Summary view in the QHN System is restricted as provided by these policies...

15) "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 and health care operations pursuant to an Electronic Commerce Agreement entered into with QHN.

16) "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, subject to acceptance by QHN. Participant Users shall be natural persons.

17) "Patient Summary" shall mean the comprehensive view of an Individual's Medical Record, consisting of PHI received from QHN Participants.

18) "Permitted Purposes" shall mean any reason for exchanging message content through the eHealth Exchange which is expressly allowed by the terms of the DURSA.

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

20) "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.

21) "QHN Policies" or "Policies" shall mean the policies of QHN, as they may be amended or added to from time to time.

22) "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.

23) "Subscription Services" shall mean those services which allow a Participant to receive those portions of an Individual's Medical Records that have been properly identified and transmitted through the QHN System, regardless of whether the Participant is identified to receive delivery by the original order associated with the Medical Record.

24) "Use" shall mean the sharing, employment, application, utilization, examination, analysis, De-identification, or commingling of PHI with other information that is held by an entity.

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

	Section 1: Audit Rights
Policy 1.0	**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 any agreement it has with QHN; access that has been made to Medical 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 and the Electronic Commerce Agreement shall provide written notice to QHN at least two (2) weeks in advance Individual. 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 number and identification of persons who will perform the audit if Participant wishes to conduct an audit at QHN facilities. 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	2) The audits will be scheduled by mutual agreement between QHN and Participant and such agreement will not be unreasonably withheld. 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 PHI or is required by applicable law.
Confidentiality Agreements	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.
Expenses Incurred	4) Each auditor acting on Participant's behalf shall sign an *ad hoc* confidentiality agreement (in addition to any other confidentiality agreements already in place) in a form acceptable to QHN prior to performing the 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 and shall only have access to information related to Medical Records placed in the QHN System

	by such Participant. 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 Reviewed: December 21, 2011; February 10, 2016

Policy 1.1	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 Policies 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	1) QHN shall provide a Participant written notice at least two (2) weeks in advance of sending persons to perform an audit. 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, number and identification of persons to perform the audit. If Participant wishes to conduct an audit at QHN facilities, 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	2) The audits will be scheduled by mutual agreement between QHN and Participant and such agreement will not be unreasonably withheld. 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 PHI or is required by applicable law.
Hours of Audit	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.
Expenses Incurred	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

Policy 1.2	STANDARD
	Participant System Use Audits/Audit Controls. Participants shall audit Participant Users' Use of, and access to, the QHN System.
	POLICY
Audit Specifications	1) QHN will record System activity and access through hardware and software mechanisms that record System activity and access to Medical Records and PHI. QHN will generate usage reports to be given to every Participant for their review. The report will show the Participant Users who accessed Individual Medical Records within the Patient Summary record of QHN. Participants are required to review the report and notify QHN's Privacy and Security Officer about any suspected unauthorized accesses to patient information.
Audit Frequency	2) This usage report may be distributed to Participants no less often than quarterly. 3) At its discretion, QHN may generate and distribute to Participants, usage reports of other applications and access to or within the QHN System. 4) 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	5) If QHN becomes aware of a Participant User's misuse of the QHN System, the Participant User and the respective Participant shall 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

Policy 1.3	STANDARD
	Immediate Audit by QHN: QHN shall have 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 needs to perform an immediate audit. 3) QHN will provide Participant with reasons necessitating the immediate audit at the time notice is provided. However, the decision to perform the immediate audit shall remain solely at the discretion of QHN. 4) Upon notice to Participant by QHN, Participant shall provide QHN access 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

Policy 1.4	STANDARD
	Audits by Government and Other Organizations: QHN shall permit audits of QHN's records to the extent allowed or 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 allowed or 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. Audit findings will be made available to QHN Participants, if determined by QHN to be appropriate.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

	Section 2: Medical Records
Policy 2.0	**STANDARD**
	Access and Amendments to Medical Records: Participant may make amendments to Medical Records as required or allowed by HIPAA. QHN shall refer any Individual requests for Access or Amendment to PHI to the appropriate Participant.
	POLICY
Requests Made to Participant by an Individual	1) If an Individual requests an amendment to an Individual's information, Medical Records or PHI in the QHN System or for access to an Individual's information, Medical Records or PHI in the QHN System, information regarding such requests shall be forwarded to the Participant by QHN.
QHN's Role	2) QHN is not authorized to directly accept requests from Individuals for amendment or access, or any other requests by Individuals to exercise other rights related to the Use or Disclosure of an Individual's information, Medical Records or PHI in the QHN System. If an Individual makes a request to QHN related to an Individual's information, Medical Records or PHI in the QHN System, the Individual will be informed that QHN is not authorized to directly accept requests from Individuals, and the Individual will be directed to make the request to the appropriate Participant. QHN will notify Participant within 5 business days, if QHN receives such a request from an Individual.
Participant's Role	3) Upon receipt of a request from an Individual for an amendment to a Medical Record that Participant has agreed to accept, Participant shall submit the amended record to QHN.
QHN not Responsible for Amendments	4) QHN shall not be responsible for making amendments to Medical Records or be responsible for providing an Individual with access to an Individual's information, Medical Records or PHI in the QHN System. 5) QHN shall not be responsible for the accuracy of any amendments made to Medical Records by Participants.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

Policy 2.1	STANDARD
	Accounting of Disclosures: QHN will provide information to a requesting Participant, collected in accordance with QHN Policies and Procedures, to permit the Participant to respond to a request by an Individual for an accounting of disclosures of Medical Records or PHI as required by law.
	POLICY
QHN Record of Disclosure	1) If QHN makes a disclosure of any Medical Records or PHI requiring an accounting of disclosure under HIPAA or other applicable laws, QHN shall maintain an accounting or record of all such disclosures of Medical Records as may be required by applicable law.
Accounting to the Participant from QHN	2) Upon receipt of a written request from a Participant for an accounting of disclosures of Medical Records or 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 or other applicable law. 4) If an Individual makes a request to QHN for an accounting of disclosures related to an Individual's information, Medical Records or 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.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

Policy 2.2	STANDARD
	Access Audit: Participant may request that QHN perform an audit of an Individual's Medical Records or PHI within the QHN system for the purpose of identifying accesses to the record.
	POLICY
Requests made to a Participant by an Individual QHN's role Participant's Role Denial and Expenses	1) To the extent an Individual requests an audit of accesses to their Medical Records or PHI in the QHN System, Individuals shall be informed that such requests shall be made to the appropriate Participant and not to QHN. 2) QHN is not authorized to directly accept requests from Individuals. QHN will notify Participant within 5 business days, if QHN receives such a request from an Individual. 3) Upon receipt of a request from an Individual, Participant shall submit the request to QHN, in accordance with QHN Procedures in place at that time. 4) QHN reserves the right to deny the access audit request and/or to assess a reasonable and appropriate fee for said audit.
Policy Dates	Written: February 10, 2016 Amended: _____ Reviewed: _____

	Section 3: Individual Consent
Policy 3.0	**STANDARD**
	Individual Consent: Individuals may request to Opt Out of the QHN System. As defined in these QHN Policies, to Opt Out shall mean that access to an Individual's Medical Records located in the Patient Summary view of the QHN System is restricted. Opt Out does not prevent medical providers from directly exchanging Medical Records within the QHN System.
	POLICY
Individual notifies Participant Participant Reviews Requests and Implements Opt Out Restrictions QHN's Role	1) An Individual's request to Opt Out of QHN shall be submitted to the appropriate Participant. The Participant will be responsible for managing and responding to the request. 2) Participant is required to grant the Opt Out request to block future access to the Individual's Patient Summary. 3) 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. Individual Participants will be provided instruction regarding how to put the Opt Out restrictions in place to block future access to the Patient Summary. 4) 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. 5) At its discretion, QHN may offer other methods for Individuals to Opt Out of the QHN System.
Policy Dates	Written: February 10, 2016 Amended: _____ Reviewed: _____

	Section 4: Subpoenas/Law Enforcement Inquiries
Policy 4.0	**STANDARD**
	Subpoena for Medical Records: QHN shall respond to subpoenas for Medical Records promptly and in conformity with HIPAA and all other applicable federal and state law.
	POLICY
Role of Executive Director	1) Subpoenas for Medical Records received by QHN shall be directed immediately to the Executive Director and acted upon appropriately.
	2) QHN will cooperate and assist Participant(s) with any required response to any subpoena to the extent allowed under applicable law.
Subpoenas and Responses are Tracked	3) QHN shall keep a log of any subpoenas for Medical Records received by QHN according to generally accepted standards for record retention. Such log shall include information such as: date subpoena was received and date Participant(s) were notified of inquiry.
	4) QHN may charge a reasonable fee associated with handling and responding to subpoena.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

Policy 4.1	STANDARD
	Law Enforcement Inquiries for Medical Records: QHN shall respond to law enforcement inquiries for Medical Records promptly and in conformity with HIPAA and all other applicable laws.
	POLICY
Role of Executive Director Inquiries and Responses are Tracked	1) Any law enforcement inquiry for Medical Records received by QHN shall be directed immediately to the Executive Director and acted upon appropriately. 2) QHN shall keep a log of any law enforcement inquiries for Medical Records received by QHN according to generally accepted standards for record retention. Such log shall include information such as: date inquiry was received and date Participant(s) were notified of inquiry. 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 Reviewed: December 21, 2011; February 10, 2016

	Section 5: Impermissible Use or Disclosure of PHI/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 PHI, related to Use or access of the QHN System, has occurred.
	POLICY
Notice to QHN QHN Hold Harmless	1) Participant will notify the QHN Privacy Officer or Executive Director, as soon as reasonably possible after becoming aware of any impermissible use or disclosure of PHI, 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 PHI. Participant shall inform QHN of procedures taken to remedy the problem. 3) Participant shall hold QHN harmless from any suit or claim alleging improper access was granted for Medical Records subject to special privacy standards.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

Policy 5.1	STANDARD
	QHN Investigation of Use or Disclosure; Notice to Participant: Upon discovery by QHN of an impermissible Use or disclosure of PHI related to use or access of the QHN System, the QHN Privacy and Security shall direct a prompt investigation and report findings to the Executive Director.
	POLICY
Notice to Privacy/Security Officer Procedures by QHN	1) Any QHN employee, agent, representative or subcontractor who discovers or learns of a potential impermissible use or disclosure of PHI, related to Use or access of the QHN System will notify the QHN Privacy/Security Officer as soon as reasonably possible.
	2) After receiving notification of an impermissible use or disclosure, the QHN Privacy/Security Officer shall conduct a prompt, complete investigation, in compliance with HIPAA. And shall take appropriate steps to mitigate any harmful effects.
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 PHI. 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 Participants	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 Reviewed: December 21, 2011; February 10, 2016

	Section 6: Behavioral Health Records
Policy 6.0	**STANDARD**
	Participant Responsibility: All Participants and Participant Users who Use the QHN System will comply with provisions in applicable law governing access to Medical Records containing information about certain conditions which are subject to special privacy 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 privacy standards or confidentiality requirements for certain Medical Records containing information on specified medical conditions, including but not limited to: alcohol and substance abuse treatment records, psychotherapy records, records involving HIV diagnoses and records regarding minors.
Participant responsibility for limiting access	2) When entering Medical Record information into the QHN System, the Participant or Participant User shall be solely responsible for taking appropriate precautions regarding access to information about certain conditions which are subject to special privacy standards or confidentiality requirements. QHN shall not have the responsibility for limiting access to such Medical Records, unless provided for by separate agreement.
QHN held harmless	3) Participant shall hold QHN harmless from any suit or claim alleging improper access was granted to Medical Records related to medical conditions or diagnoses that are subject to special privacy standards or confidentiality requirements.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

	Section 7: System Access and Use	
Policy 7.0	**STANDARD**	
	Participant Enrollment: A Participant shall be required to complete QHN enrollment processes and agreements before a Participant or Participant User may access and Use the QHN System.	
	POLICY	
Participants enroll with QHN	1)	A Participant shall complete enrollment materials 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 to the QHN System.
Changes in Participants Users Access	3)	Any requested change in the status of a Participant User's access to the QHN System will be submitted by Participant to QHN in a form approved by QHN.
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 have access to the QHN System or (b) may deny any Participant's request to add Participant Users; and (c) 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 review credentials, licensure, or other information.
Notify QHN of Termination or Status Change	6)	As soon as reasonably possible following termination of a Participant User's relationship with Participant (e.g.: termination of employment), Participant will notify QHN.
	7)	Upon receipt of notification of termination of a Participant User's relationship with Participant, QHN shall disable access and inform Participant.
	8)	Each Participant shall notify QHN immediately of any change in privilege, licensure or employment status of any Participant User employed by the Participant who is granted access to the System. Each Participant User who is granted access to the System shall notify QHN immediately of any change in privilege, licensure or employment status of the Participant User. Notwithstanding any provision of QHN's Policies or agreements, QHN in its sole

	discretion reserves the right to require conditions it deems appropriate for any granted Use of the System. 9) All Participant Users shall pay the applicable fees, as required by QHN, for its 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 Reviewed: September 15, 2010; December 21, 2011; February 28, 2014 (DT) ; February 10, 2016

Policy 7.1	STANDARD
	Participant Training: All Participants are required to provide HIPAA privacy and security training for all Participant Users and are strongly encouraged to attend training by QHN for the proper Use of the QHN System.
	PROCEDURE
HIPAA Training Required	1) Participant must affirm that each Participant User has received HIPAA privacy and security training before access to QHN is granted. 2) Upon request, Participant will provide documentation of such training to QHN.
Compliance with QHN Policies	3) By Use of the QHN System, each Participant User agrees to comply with QHN Policies and Standards.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

Policy 7.2	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, HIPAA and QHN Policy.
	POLICY
Access Level Assigned by QHN	1) Participant Users will be assigned a level of system access, based upon the user information provided by the Participant and as approved by QHN. Participants will only request access for those persons who need to access PHI 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 needed and any conditions appropriate to such access.
QHN Approves any Change in Access	2) Requests for change in a Participant User's level of system access shall be submitted to QHN and is subject to approval/disapproval by QHN. 3) At its discretion, QHN may 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 Reviewed: December 21, 2011; August 14, 2013; February 10, 2016

Policy 7.3	STANDARD
	Participant Use of QHN System: Use of the QHN System, by a Participant and all Participant Users, must be in compliance with HIPAA and all applicable federal or state law and consistent with QHN Policies.
	POLICY
Use of QHN System	1) QHN, Participants and Participant Users shall Use the QHN System in a manner that is compliant with HIPAA, all applicable federal or state law and consistent with QHN Policies. 2) By accessing the QHN System, Participants and Participant Users affirm compliance with Participant's Electronic Commerce Agreement with QHN and these Policies 3) It is the responsibility of the Participant and each Participant User to assure all accesses to the QHN System are in compliance with HIPAA, all applicable federal or state law, all terms and conditions of these QHN Policies, and the Electronic Commerce Agreement with QHN.
Notification of Inappropriate Access	4) Inappropriate access of 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: 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. 5) QHN may report any inappropriate access to the QHN System by a Participant User to the appropriate licensing agencies with whom the Participant User is licensed and/or to other organizations that a Participant User has a relationship or privileges with that are likely to allow the Participant User to have access to PHI.
Notification Costs Paid by Participant	6) If QHN is required by law to provide notifications to any Individual(s), other Participants, and/or any governmental entity of inappropriate access to the System by a Participant User or any person who accesses the System through Participant's right of access, the Participant shall pay all QHN's reasonable notification costs and all costs of investigating and mitigating any harmful

	effects caused by the inappropriate access.
Participant to Review Usage Reports	7) Participant shall review any and all usage reports provided to Participant by QHN. Participant must have audit policies for the review of System usage by Participant Users which are in compliance with HIPAA and all applicable federal or state law. Participant shall have a sanctions policy that meets the minimum HIPAA standards.
Sanctions for Misuse	8) Any Use of the QHN System by QHN, a Participant or Participant User that is contrary to QHN Policies, Electronic Commerce Agreements, any applicable law, regulation or government policy, is prohibited. Sanctions 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.
Policy Dates	Written: Aug 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

Policy 7.4	STANDARD
	Participant and Participant User Responsible for Accurate Delivery of PHI: Participant and Participant Users are responsible for notifying QHN of current routing information in order to assure accurate and appropriate delivery of PHI.
	POLICY
Participant Users Responsible for Accurate Delivery	1) Participant 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 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 PHI will be maintained and Used in compliance with HIPAA.
Policy Dates	Written: April 17, 2013 Amended: February 10, 2016 Reviewed: February 10, 2016

	Section 8: Subcontractor/Agent/Other Contracted Organizations
Policy 8.0	**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 the same restrictions and conditions regarding Use of the QHN System that apply to QHN under Business Associate Agreements to which QHN is a party.
	POLICY
Agreement Required	1) QHN shall require subcontractors, agents or other organizations who will have access to the QHN System to enter into HIPAA compliant confidentiality agreements with QHN. Such agreement will contain the same restrictions and conditions applying to QHN in any Business Associate Agreement to which QHN is a party, including a provision that prohibits Use or disclosure of PHI other than is allowed by applicable law.
	2) Subcontractors, agents or other contracted organizations will not have access to the QHN System until such agreement is fully executed.
Possible Sanctions	3) Failure or alleged failure of a QHN subcontractor, agent or other contracted organization to comply with QHN Policies or any written agreement with QHN may result in an investigation and possible sanctions.
Responsible for Damages	4) 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	5) Prior to any subcontractor, agent or other contracted organization providing services related to the QHN System, such organizations shall conduct background checks on employees of subcontractor, agent or contracted organization who may have more than incidental access to PHI in the QHN System.
System Security is Compliant/Safeguards in Place	6) All subcontractors, agents or other contracted organizations that are providing managed hosting, software, and/or other technological services related to the QHN System shall maintain all administrative, physical and technical safeguards required by HIPAA, all applicable federal and state law, and QHN Policies.
Privacy Policies Compliant with HIPAA	7) Every subcontractor, agent or other contracted organization shall maintain privacy and security policies as required by HIPAA, all applicable federal and state law, and QHN Policies.

Confidentiality	8) 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 PHI on the QHN System confidential; B. Hold all QHN proprietary information confidential; and, C. Have completed HIPAA Privacy and Security Training.
Security Audits Upon Request	9) 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, all federal and state law, and QHN Policies.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

	Section 9: System Access – Non Participant
Policy 9.0	**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.
	POLICY
	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, Electronic Commerce Agreements, all applicable federal and state law, QHN Policies, and any privacy and security requirements defined by QHN.
Policy Dates	Written: February 10, 2016 Amended: _____ Reviewed: _____

	Section 10: Participant Subscription
Policy 10.0	**STANDARD**
	Subscription Services: QHN may provide Participants with Subscription Services for Individuals with whom Participant has a relationship for purposes of "treatment," "payment" or "health care operations" activities, as defined by HIPAA. Individual Medical Records
	POLICY
Execution of Agreement	1) Participant shall execute the appropriate agreement provided by QHN prior to QHN providing Subscription Services to Participant.
	2) Participant is responsible for maintaining an accurate record of all Individuals for whom Subscription Services are provided.
	3) Subscription Services for a Participant may include extraction of an Individual's Medical Records, as directed by the Participant
Notice to QHN	4) Participant must notify QHN of any changes to those subscribed Individuals that Subscription Services are no longer needed because Participant no longer has a relationship with the Individual for purposes of "treatment," "payment" or "health care operations" activities. Notice by the Participant must be given as soon as possible, and shall in every case be given within thirty (30) days of the change.
	5) 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.
	6) Subscription Services for a Participant may exclude Medical Records of an Individual who has chosen to Opt Out of the QHN System.
	7) Subscription Services for a Participant may exclude Medical Records that are governed by special privacy standards or confidentiality requirements that restrict the disclosure of such Medical Records.
Policy Dates	Written: February 10, 2016 Amended: _____ Reviewed: _____

	Section 11: Data Integrity
Policy 11.0	**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 consistent with TPO	1) All information placed in the QHN System shall comply with QHN requirements regarding placing information in the QHN System.
Exceptions to TPO require QHN approval	2) The data that is placed in the QHN System shall be consistent with the purposes of treatment, payment and health care operations. Data not relating to treatment, payment and health care operations shall not be placed in the QHN System without the express written consent of QHN. 3) QHN may allow data regarding the social determinants of the health of the Individual to be placed in the QHN System.
Possible Sanctions	4) 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 Reviewed: December 21, 2011; February 10, 2016

	Section 12: Research
Policy 12.0	**STANDARD**
	Research Request Procedures: QHN shall allow for and consider data requests for research purposes. No research request may be approved without approval of the Board of Directors as described below. 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.
	POLICY
Requests of data for research purposes	1) All requests of 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 contained on the QHN Research Request Form, a copy of which can be found in the "Supplemental Information" section at the end of the 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 each research request: A. Deny the research request; B. Submit the request to the Board of Directors for final

Majority vote of review committee is needed	review with a recommendation for approval or denial; or C. Submit the request to a review committee established by the Board of Directors, for recommendations, prior to submission to the Board of Directors. 3) If the request is submitted by the Executive Director to a committee of the Board of Directors, majority vote of the referenced committee will determine the recommendation to the Board of Directors.
Approval	4) Unanimous approval by all members of the Board of Directors is required for 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. 5) 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.
Policy Dates	Written: August 25, 2005 Amended: January 15, 2014; February 10, 2016 Reviewed: December 21, 2011; January 15, 2014; February 10, 2016

Policy 12.1	STANDARD
	Data Must be De-identified: QHN will not allow any data that is not De-identified or in a limited Data Set to be used for research purposes, except under certain circumstances.
	POLICY
Data retrieved by QHN	1) Board of Directors' approved data research projects will be delegated to the Executive Director for assignment to QHN employee(s) who will retrieve the data. 2) Any and all data for approved data research projects will be compiled only by QHN or its designee.
Data De-identified	3) Except as provided in paragraph 4 below, all data for research projects will be De-identified of PHI or will meet HIPAA requirements for limited data set disclosures (i.e. 45 C.F.R. 164.514(e)), prior to being given to the requesting entity. Disclosure of a limited data set may only occur pursuant to a HIPAA compliant "Data Use Agreement" approved by the Executive Director."
Exceptions	4) As an exception to the requirement to provide only De-Identified data or a "limited data set", PHI may be disclosed if the following requirements are met: A. Such Use and Disclosure is unanimously approved by the QHN Board of Directors, 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 Reviewed: December 21, 2011, January 15, 2014; February 10, 2016

	Section 13: Sanctions
Policy 13.0	**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
QHN discovers non compliance Temporary restrictions Notices and Responses in Writing Executive Director determines sanction Report to licensing authority possible	1) Where QHN discovers noncompliance by a Participant or Participant User, as soon as reasonably possible, the QHN Executive Director or Privacy/Security Officer shall notify the Participant of the issue in writing. 2) QHN reserves the right to restrict access to the QHN System at the time of discovery, pending further investigation. 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. 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). 6) Sanctions of Participants and Participant Users shall concern inappropriate use of the QHN System by Participants and Participant Users. Such 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 future use of the QHN System, and sending notice to the appropriate licensure board and other organizations that a Participant or Participant User has a relationship or privileges with that are likely to allow the Participant or Participant User to have access to PHI. 7) QHN shall provide notice of a sanction to the Participant and Participant User and to the QHN Board of Directors 8) Participants or Participant Users may request an appeal to review

Right to Appeal	the sanctions. Written appeal for review of sanctions must be received by the QHN Board of Directors within five (5) business days of notification of the sanction.
Role of the Board	9) The Board of Directors shall schedule a meeting to review the written appeal of the sanction(s). The Participant and Participant User have the right to appear at the board meeting to present the Participant and Participant User's position regarding the appeal. The Board of Directors decision on the appeal shall be final.
Executive Director retains the right for immediate action to sanction	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 Medical Records are in the QHN System. In such a circumstance, the Executive Director will conduct an investigation as soon as reasonably possible. 11) There is no requirement that QHN or the Executive Director use this sanction process in instances in which QHN is enforcing its rights under an agreement with a Participant or Participant User, protecting the rights of a Participant, Participant User or Individual or enforcing QHN Policies.
Policy Dates	Written: August 25, 2005 Amended: December 10, 2008; December 21, 2011; February 10, 2016 Reviewed: December 10, 2008; December 21, 2011; February 10, 2016

Policy 13.1	STANDARD
	Employee Sanctions: Failure or alleged failure of a QHN employee to comply with QHN Policies, 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 Policy, applicable law, or any written or oral agreement between the employee and QHN may result in disciplinary action for the employee, up to and including termination. 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 Reviewed: February 10, 2016

	Section 14: HIPAA Compliance
Policy 14.0	**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 and Medical Records. 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 in order 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 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 Reviewed: December 21, 2011, April 17, 2013; February 10, 2016

Policy 14.1	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.
	POLICY
Disaster Recovery Plans in Place	1) QHN shall create a Disaster Recovery Plan to restore any loss of data, Data Backup Plan to create and maintain retrievable copies of electronic PHI 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 will be reviewed periodically and in response to material changes effecting the security of PHI 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 an applications and data criticality analysis.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed: February 10, 2016

Policy 14.2	
	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 to Facility	1) All visitors at a QHN facility shall register upon entry or shall be accompanied by a QHN staff member during the visit. 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 shall be locked and secured outside of normal business hours. 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

Policy 14.3	STANDARD
	Workstation Security; Encryption: QHN employees shall follow QHN's workstation security procedures to minimize unauthorized access to PHI 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.
	2) Employees shall not store any PHI, 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 PHI in any work area.
Portable Devices	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.
Removable Media	5) Unless approved by the Executive Director or his designee, no PHI, 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.
No Third Party Access	6) QHN shall ensure that third parties are not given access to or use of QHN office equipment containing PHI 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

Policy 14.4	STANDARD
	Use of Technology; Workstation Use: Every QHN employee shall follow QHN procedures for use of technology to minimize unauthorized access to PHI 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 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

Policy 14.5	STANDARD
	Equipment Repair/Disposal/Tracking: QHN Equipment containing PHI 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 PHI or other sensitive data will be conducted in accordance with HIPAA security requirements, including, but not limited to, removal of all PHI prior to shipping. Additional related requirements and detail are provided in the QHN Employee Handbook, which is incorporated here by reference. 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 PHI. 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. 3) Any computer hardware or computing equipment containing or storing PHI shall be appropriately destroyed and electronic PHI must be completely removed when such equipment is no longer used or is disposed of.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed: February 10, 2016

Policy 14.6	STANDARD
	QHN System Security Evaluation, Audits and Risk Analysis: QHN shall conduct security evaluations, audits, and risk analysis (collectively "Reviews") regarding that portion of the QHN System that is located on-site at a QHN facility or in locations under QHN's control. The security Reviews will be conducted in compliance with the requirements of HIPAA and to ensure the integrity, confidentiality and availability of information and resources in the QHN System.
	POLICY
Scope	1) The security Reviews will cover those portions of the QHN System that are under the control of QHN and will be in compliance with HIPAA and other security regulations, as may change from time to time. 2) QHN's security management process shall require implementation of Procedures designed to prevent, detect, contain, and correct security incidents and violations.
Frequency	3) 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 risks to PHI; B. Review of records of information system activity, such as audit logs, access reports, and logs of security incidents. C. Developing plans to implement or modify security measures to reasonably and appropriately address and reduce the risks identified in the Review; and D. 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

Policy 14.7	STANDARD
	Participant System Security Requirements: Each Participant shall maintain appropriate administrative, physical and technical safeguards that are reasonably designed to protect the confidentiality, integrity and availability of PHI in the system used by Participant or Participant User to access the QHN System, in accordance with HIPAA and other applicable law.
	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 each 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 Reviewed: February 10, 2016

Policy 14.8	STANDARD
	Communication Between Participant Users and QHN System: All communication containing PHI, between Participant Users and QHN shall be secured in accordance with HIPAA and all other applicable laws.
	POLICY
Secured Access Secure Transmission	1) Access to the QHN System may be via web services using secure internet browsers or other secure services. 2) Participants and Participant Users do not access QHN servers by direct connection. 3) Transmissions are protected, using generally accepted encryption Standards, data integrity controls, or other secure standards, in accordance with HIPAA and other applicable laws.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed: February 10, 2016

	Section 15: Employee Clearance/Training
Policy 15.0	**STANDARD**
	Background Checks Required: QHN shall conduct a background check for all employees hired by QHN. Employee access to the QHN System, PHI, 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 and drug screen 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, PHI, 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

Policy 15.1	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. 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 Reviewed: February 10, 2016

Policy 15.2	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.
Review and audit	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 policies.
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

	Section 16: Passwords/User ID/User Workstation
Policy 16.0	**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	1) QHN determines and assigns a unique User ID for each User, and establishes appropriate and secure password configuration requirements for access to the QHN System. QHN may require that passwords be regularly and periodically changed or reset at any time.
User Creates Unique Password	2) Users are responsible for creating and securing their unique password. 3) 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. 4) If a User suspects that their password has been compromised, the User shall immediately reset their password and notify QHN.
QHN May Disable User ID and Password	5) QHN retains the right to disable the User ID and password if QHN determines that inappropriate use of the System has occurred. 6) Misuse of a User ID or password may result in Sanctions being imposed by QHN, as outlined in these policies.
Policy Dates	Written: August 25, 2005 Amended: December 21, 2011; February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

Policy 16.1	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.
	POLICY
Unique Log In ID Single Sign On	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.
Attestation	2) An attestation in a form acceptable to QHN may also be required. In addition to other requirements, the attestation shall contain the following requirements regarding the Participant's system:
Passwords	A. The Single Sign On functionality, requires that Participant Users will at all times utilize unique log-in ID's, passwords, and other security requirements for the Participant's electronic system that are at least equal to or greater than the QHN requirements for Use of the QHN System. QHN's requirements for Use of the QHN System are set forth in the QHN Standards. B. The Participant's policy for log-in ID's and passwords shall require that each of the Participant Users has a unique Log-in ID and password that is not shared with other Participant Users.
Policy Dates	Written: April 17, 2013 Amended: February 10, 2016 Reviewed: February 10, 2016

Policy 16.2	STANDARD
	Secure Workstation: Each User shall maintain physical control of the workstation that is used for access of the QHN System
	PROCEDURE
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

	Section 17: Confidentiality Agreements
Policy 17.0	**STANDARD**
	QHN Employee Confidentiality: All QHN employees shall enter into confidentiality agreements with QHN, as required by QHN.
	POLICY
	1) For details as to the terms and conditions of the QHN employee confidentiality agreement, refer to the QHN Employee Handbook.
Policy Dates	Written: August 25, 2005 Amended: February 10, 2016 Reviewed: December 21, 2011; February 10, 2016

Policy 17.1	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 Medical 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 things 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

	Section 18: DURSA Requirements
Policy 18.0	**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 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.
Policy Dates	Written: August 17, 2011 Amended: _____ Reviewed: December 21, 2011; February 10, 2016

Policy 18.1	DURSA STANDARD
	DURSA Breach Notification: QHN and DURSA Participants shall comply with the breach notification requirements under the DURSA
	PROCEDURE
	1) Within one (1) hour of discovering information that leads a DURSA Participant to reasonably believe that a breach has occurred, the DURSA Participant shall alert QHN of the discovery and will assist and cooperate with QHN in providing notifications as required under the DURSA. 2) As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a breach 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 and the eHealth Exchange Coordinating Committee or its designee of the breach. 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: _____ Reviewed: December 21, 2011; February 10, 2016

Policy 18.2	DURSA STANDARD
	QHN and DURSA Participant Requirements: QHN and DURSA Participants shall comply with all other requirements of the DURSA. The requirements of the standard shall be incorporated into all newly issued electronic commerce agreements entered into between QHN and Participants.
	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 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 a breach 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: _____ Reviewed: December 21, 2011; February 10, 2016

Policy 18.3	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, 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 Section 12.01(b) of the DURSA.
Policy Dates	Written: December 21, 2011 Amended: _____ Reviewed: February 10, 2016

	Section 19: QHN Policy Compliance Review
Policy 19.0	**STANDARD**
	QHN Policies Reviewed Periodically: QHN shall periodically audit both its compliance with the QHN Policies, as well as the adequacy of the QHN Policies.
	POLICY
Scope Frequency	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.
Policy Dates	Written: December 21, 2011 Amended: February 10, 2016 Reviewed: February 10, 2016

SUPPLEMENTAL INFORMATION

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