Georgia Health Information Network, Inc. Georgia ConnectedCare Policies

Version History

Effective Date: August 28, 2013	**Revision Date:** August 2014
Originating Work Unit: Health Information Technology – Health Information Exchange	**Revision Number:** 1

TABLE OF CONTENTS

Georgia ConnectedCare Services – Policy Number: GaHIN-1000
Policy Title: Introduction

Who Must Comply with the Policies and Procedures

All Network Participants who have been accepted by Vendor and Network Facilitator for participation in the Network as a Network Participant and have entered into a written agreement with Vendor concerning the Network Participant's use of the Network, are required to comply with these Policies. In addition, all Network Participants must require their Member Affiliates to comply with these Policies.

Where appropriate, or where required by the operational models and/or governance structures of the Network Participant, a Network Participant may delegate certain of the responsibilities set forth in the Policies to its Member Affiliates.

These Policies apply to Health Data (including Health Care Provider Health Data, Health Plan Health Data, and HIO Health Data), as defined herein, that is exchanged via the Network.

GLOSSARY

Applicable Law shall mean all applicable statutes, rules and regulations of the State of Georgia, as well as all applicable federal statutes, rules, and regulations, including without limitation, HIPAA, HITECH, the Minimum Necessary Standard, and 42 C.F.R. Part 2 ("Confidentiality of Alcohol and Drug Abuse Patient Records").

Authorized User means a member of the Workforce of a Network Participant or a Member Affiliate who has been designated by that Network Participant or Member Affiliate to access the Network pursuant to the concept of role-based access control. An Authorized User may also be a member of Network Facilitator's or Vendor's Workforce; or a member of the Workforce of a Business Associate of Network Facilitator or Vendor.

Breach "Breach" shall be defined to be the unauthorized acquisition, access, use or disclosure of Protected Health Information disclosed through the Network in a manner not permitted under Subpart E of 45 C.F.R. § 164.402, as may be amended, which compromises the security or privacy of the PHI. A Breach is also defined as a DURSA Breach.

> **DURSA Breach** is a subset of Breach and shall mean the unauthorized acquisition, access, disclosure, or use of Message Content (which includes Protected Health Information, de-identified data, individually identifiable information, pseudonymized data, metadata, schema, and digital credentials) while sending, requesting, receiving, responding to, or otherwise exchanging or disclosing Health Data via the eHealth Exchange, or the nationwide health information network. "DURSA Breach" does not include the following: (1) any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Network Participant or Member Affiliate if: (a) such acquisition, access, disclosure or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Network Participant or Member Affiliate; and (b) such Message Content is not further acquired, accessed, disclosed, or used by such employee or individual; or (2) any acquisition, access, disclosure or use of information contained in or available through the Network Participant's systems where such acquisition, access, disclosure or use was not directly related to sending, requesting, receiving, responding to, or otherwise exchanging or disclosing Message Content via the eHealth Exchange.

Business Associate shall have the meaning set forth at 45 C.F.R. § 160.103.

Business Associate Agreement means a contract between a Covered Entity under HIPAA and a Business Associate, or between Business Associates, which obligates the Business Associate to

maintain the privacy and security of Protected Health Information in accordance with the requirements of the HIPAA Regulations.

Covered Entity shall have the meaning set forth at 45 C.F.R. § 160.103.
Designated Record Set shall have the meaning set forth at 45 C.F.R. § 164.501.

DURSA shall mean the eHealth Exchange Data Use and Reciprocal Support Agreement entered into by Network Facilitator.

Health Care Operations shall have the meaning set forth at 45 C.F.R. § 164.501.

Health Care Provider shall have the meaning set forth at 45 C.F.R. § 160.103.

Health Care Provider Health Data shall mean only that Health Data that is, or could reasonably be expected to be, useful for Treatment, Payment, and Health Care Operations, all in accordance with HIPAA Regulations.

Health Data shall mean any of that electronic healthcare related information that is disclosed through, made available on, or sent through the Network. Health Data shall include, but may not be limited to, Health Care Provider Health Data, Health Plan Health Data, and HIO Health Data, and includes Protected Health Information.

Health Information Exchange means a system for the electronic transfer of Protected Health Information between participating organizations for a permissible purpose based upon the requirements of federal and state law.

Health Information Organization or **HIO** shall mean an organization that oversees and governs the exchange of health-related information, other than the Network Facilitator.

Health Plan shall have the meaning set forth at 45 C.F.R. § 160.103.

Health Plan Health Data shall mean that Health Data that includes admission, discharge, and transfer data of Patients covered by the Health Plan requesting such data and such other Health Data as approved in writing by a majority of the Network Participants, in accordance with HIPAA Regulations, including the Minimum Necessary Standard.

HIO Health Data shall mean that Health Data that is, or could reasonably be expected to be, useful for Treatment, Payment, or Health Care Operations, all in accordance with HIPAA Regulations.

HIPAA shall mean the Health Insurance Portability and Accountability Act of 1996, as amended by HITECH, as currently in effect and as may be amended, modified, or renumbered.

HIPAA Regulations shall mean the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160, 162 and 164) promulgated by the U.S. Department of Health and Human Services under HIPAA, and any amendments.

HITECH shall mean the Health Information Technology for Economic and Clinical Health Act of 2009 (which is part of the American Recovery and Reinvestment Act of 2009 (45 C.F.R. Part 495)), as amended, and any of its implementing regulations.

Individually Identifiable Health Information shall have the meaning set forth at 45 C.F.R. § 160.103.

Master Patient Index means the index wherein Personal Demographic Information of Patients is securely maintained by the Network to record their decision to Opt-Out of the Network. For those Patients who have not elected to Opt-Out, the Master Patient Index shall be used to match the Patients

with any inquiries seeking the exchange of Protected Health Information for a Permitted Purpose. The Network shall maintain Personal Demographic Information regarding all potential individual Patients in this Master Patient Index, even if the decision is made to Opt-Out, in order to minimize the possibility of improperly matching Patients.

Member Affiliates shall mean those persons who have been authorized by a Network Participant to access Health Data through the Network and in a manner defined by such Network Participant, in compliance with the terms and conditions of the Member Agreement and Applicable Law.

Member Agreement shall mean that certain agreement entered into by and between the Network Facilitator for statewide health information exchange services, and Network Participant, as may be amended and/or restated from time to time.

Minimum Necessary Standard shall mean the "minimum necessary standard" as set forth in 45 C.F.R. § 164.502(b) and 45 C.F.R. § 164.514(d), as the same may be amended from time to time.

Network shall mean the network that allows for the electronic exchange of Health Data between and among Network Participants and their respective Member Affiliates as described in the Member Agreement.

Network Facilitator shall mean the Georgia Health Information Network, Inc.

Network Participant shall mean any organization that (i) is a Health Care Provider, Health Plan, State Agency, or Health Information Organization; (ii) meets the requirements for participation in the Network as contained in the Network Operating Policies and Technical Requirements; (iii) is accepted by Vendor and Network Facilitator for participation in the Network as a Network Participant, and (iv) has entered into a written agreement with Vendor governing such Network Participant's use of the Network, including Member. "Network Participant" shall mean "Qualified Entity" for purposes of the Vendor Contract.

O.C.G.A. shall mean the Official Code of Georgia Annotated.

Opt-Out means a process under which any Patient who does not wish to have his or her Health Data exchanged with other Network Participants pursuant to the Network may affirmatively express his or her decision not to participate.

Patient means the individual whose Personal Demographic Information or Protected Health Information is subject to electronic storage and transfer by the Network. "Patient" includes a personal representative who has the authority to authorize the disclosure of a Patient's Protected Health Information pursuant to 45 C.F.R. § 164.502(g) and any other Applicable Law.

Payment shall have the meaning given such term at 45 C.F.R. § 164.501.

Personal Demographic Information means information which may be used to individually identify a Patient, and may include, but not be limited to, name, address, Social Security number, date of birth, telephone number, and driver's license number.

Protected Health Information shall have the meaning set forth at 45 C.F.R. § 160.103, and may also be referred to as PHI.

Required By Law shall have the meaning set forth at 45 C.F.R. § 164.103.

Sensitive Health Information shall mean drug and alcohol records as defined by 42 C.F.R. Part 2; genetic information as defined by O.C.G.A. § 33-54-2; mental health records as defined by 45 C.F.R. § 164.508(a)(2) and 45 C.F.R. § 164.501 and O.C.G.A. §§ 43-39-16, 37-3-166, 37-1-1; HIV/AIDS information as defined by O.C.G.A. §§ 31-22-9.1, 24-12-20, and 24-12-21 ; and mental retardation

records as defined by O.C.G.A. §§ 37-4-125 and 37-1-1(8). Sensitive Health Information may also be referred to as SHI.

State Agency shall have the meaning set forth in O.C.G.A. § 50-5-82(a).

Suspected Breach shall refer to, for purposes of the Breach Notification Policy, the point at which either the Network Facilitator, Vendor, Network Participant, or Member Affiliate discovers information that leads it to reasonably believe that a Breach may have occurred.

Unsecured PHI shall have the meaning set forth at 45 C.F.R. § 164.402.

Treatment shall have the meaning set forth at 45 C.F.R. § 164.501.

Workforce has the same meaning as the term is defined in 45 C.F.R. Part 160, as may be amended.

Georgia ConnectedCare Services – Policy Number: GaHIN-1001

Policy Title: Data Practices of Georgia Health Information Network, Inc. ("GaHIN") for Query-Based Services, currently marketed by GaHIN as Georgia ConnectedCare.

PURPOSE: This Policy defines how Network Facilitator's Query-Based Exchange Services interacts with Health Data.

SCOPE: This policy applies to the Network Facilitator's Query-Based Exchange Services.

DEFINITIONS: Query-Based Exchange Services – For the purpose of this policy Query-Based Exchange Services is a secure service that allows Network Participants and Member Affiliates to search and locate a specific patient's information.

POLICY: Network Facilitator and its vendor(s) do not in any way access, use, or disclose, Health Data, except as required for the maintenance of Personal Demographic Information retained in the Master Patient Index (MPI) or for the purposes of supporting the system or system users. Health Data exchanged by Network Participants and Member Affiliates must be encrypted and secured according to the technical specifications approved by Network Facilitator that satisfy the HITECH Rules for secured PHI and minimize the impact of any data breach.

Access to Health Data transmitted, sent, or received through the Network is limited to Network Participants and Member Affiliates identified by the Network Participant. Network Facilitator and its contractors and vendors cannot decrypt and cannot access Health Data transmitted, sent, or received through the Network.

Georgia ConnectedCare Services – Policy Number: GaHIN-1002
Policy Title: Identity Verification

PURPOSE: The purpose of this Policy is to ensure that only appropriate and specifically authorized individuals gain access to the Network, and to prevent unauthorized access to Health Data that is exchanged through the Network.

SCOPE: This Policy applies to the Vendor and all Network Participants and Member Affiliates in the Network.

POLICY: Access to the Network is restricted to authorized Network Participants and Member Affiliates. All Authorized Users must be authenticated prior to accessing Health Data through the Network. It is anticipated that the following individuals may become an Authorized User: 1) Workforce members of any Network Participant or Member Affiliate; 2) Workforce members of the Network Facilitator; and 3) Workforce members of the Network Facilitator's Business Associates. Before any of the above individuals may be granted access to the Network, they must be properly designated as an Authorized User.

Initial Network Participant authentication shall be performed by the Vendor in accordance with the documentation and verification requirements set forth in the Digital Certificate Policy. (See Policy 1010). Upon subsequent access to the Network, Network Participants will be prompted to authenticate their identity.

Each Network Participant is responsible, in accordance with its own policies and procedures, for verifying the identities of Authorized Users of its own Member Affiliates for purposes of accessing Health Data through the Network from the Network Participant's System. A Network Participant that is a Health Information Organization may delegate this responsibility to its Member Affiliates. Such identity verification may be conducted through review of documentation, such as a government-issued identification card, social security card, Member Affiliate provider number (if applicable), or other documentation in accordance with the Network Participant's own internal identity verification policies and procedures. The Network Facilitator will require compound single-factor authentication, which will be based upon at least 2 things that an Authorized User uniquely knows (e.g., username and password). An Authorized User will have to utilize both aspects of his or her authentication information in order to be granted access to the Network. Should legal requirements ever impose the need for two-factor authentication, the Network Facilitator will establish procedures to ensure compliance with such laws.

In accordance with the Network Facilitator's Network Participant Terms and Conditions, each Network Participant shall have written policies and procedures in place that govern its Member Affiliates' ability to access information on or through the Network Participant's System and through the Network ("Network Participant Access Policies"). The Network Facilitator acknowledges that Network Participant Access Policies will differ among Network Participants as a result of differing Applicable Law and business practices. As specified in the Network Participant Terms and Conditions, each Network Participant must have a written agreement with each of its Member Affiliates, and/or policies and procedures specifying that Member Affiliates are required to comply with the Member Agreement and Applicable Law, and which ensure that Health Data is requested and viewed by a Member Affiliate with the legal authority to have such access.

The status of an Authorized User can change. The Network Facilitator must rely upon its Network Participants and Member Affiliates to update the Network Facilitator so that Authorized User status can be terminated or amended, as necessary. Similarly, the Network Facilitator must rely upon its Network Participants, Member Affiliates and Business Associates to educate and oversee their Workforce to ensure that this User Authentication Policy is consistently followed. Any and all violations must be reported to the Network Facilitator promptly so that appropriate safeguards can be taken to eliminate or mitigate the possibility of access to the Network by any unauthorized individual.

Georgia ConnectedCare Services – Policy Number: GaHIN-1003
Policy Title: Notice of Privacy Practices

PURPOSE: This policy is intended to ensure that all Network Participants and Member Affiliates develop, maintain, and appropriately distribute Notices of Privacy Practices (NPPs) consistent with applicable federal and state laws.

SCOPE: This Policy applies to all Network Participants and Member Affiliates.

POLICY: Each Network Participant, where applicable, and Member Affiliate shall develop, distribute, and maintain an NPP that complies with all Applicable Laws and this Policy. As further explained in the Opt-Out Policy (see Policy Number 1007), a Network Participant's and Member Affiliate's NPP may contain a notice of the Patient's right to Opt Out of having his or her Health Data exchanged via Health Information Exchange.

The NPP shall meet the content requirements set forth under the HIPAA Regulations and comply with all Applicable Law. The Network Participant or Member Affiliate will make available its NPP to a Patient prior to sending, uploading, and otherwise distributing any of the Patient's Health Data through the Network. Each Network Participant, when applicable, Member Affiliate shall implement its own procedures governing distribution of the NPP to a Patient, which shall be consistent with this Policy in accordance with Applicable Law, including HIPAA and HITECH.

For Network Participants and Member Affiliates who are Health Care Providers the NPP shall be:

- Provided to a Patient at the first date of service by the Health Care Provider;
- Made available to the public upon request;
- Made available electronically through the Network Participant's or the Member Affiliate's website (if any);
- Made available at the Network Participant's or the Member Affiliate's treatment location; and
- Posted in a clear and prominent location where it is reasonable to expect Patients seeking treatment services to be able to access the NPP.

Each Network Participant and Member Affiliate who is a Health Care Provider must make a good faith effort to obtain the Patient's written acknowledgement of receipt of the NPP or to document their efforts and/or failure to do so. Each Network Participant, when applicable, and Member Affiliate shall implement its own procedures governing obtaining written acknowledgement, which shall be consistent with Applicable Law, including HIPAA and HITECH.

A Network Participant or Member Affiliate, as applicable, must promptly revise and distribute its NPP as required by Applicable Law whenever there is a material change to the legal requirements governing the uses or disclosures, the Patient's rights, the Covered Entity's legal duties, or other privacy practices stated in the NPP.

REFERENCES: The HIPAA Privacy Rule (45 C.F.R. § 164.520).

Georgia ConnectedCare Services – Policy Number: GaHIN-1004

Policy Title: Minimum Necessary and User Authorization

PURPOSE: To ensure that reasonable efforts are made to limit the Health Data transmitted via the Network to the minimum amount necessary to accomplish the intended purpose for which the Health Data is accessed, thereby allowing Patients to have confidence in the privacy of their Health Data as it moves among Network Participants and Member Affiliates via the Network.

SCOPE: This policy applies to all Network Participants and Member Affiliates.

POLICY: Each Network Participant and Member Affiliate shall have reasonable Minimum Necessary policies and procedures to limit how much Health Data is used, disclosed, and requested for certain purposes. These Minimum Necessary policies and procedures should limit who has access to Health Data and under what conditions based on job responsibilities and the nature of the business.

1. Uses

a. Use of Health Data must be limited to the minimum amount necessary to accomplish a specified Permitted Purpose.

b. Each Network Participant and Member Affiliate shall share Health Data obtained through the Network and allow access to such information by only those Workforce members, agents, and contractors who need the information in connection with their job function or duties.

2. Disclosures

a. Each Network Participant and Member Affiliate shall disclose through the Network only the minimum amount of Health Data as is necessary for the purpose of the disclosure.

b. Disclosures to a Health Care Provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

3. Requests

a. Each Network Participant and Member Affiliate shall request only the minimum amount of Health Data necessary for the intended purpose of the request.

b. This Policy does not apply to requests by Health Care Providers for treatment purposes. To the extent that Health Data is disclosed for Treatment and some other purpose, this Policy applies.

4. Role-Based Access Standards

a. Each Network Participant and Member Affiliate shall implement a role-based access system, whereby Authorized Users may include only those members of the Network Participant's or Member Affiliate's Workforce who require access to the Network to facilitate the use and disclosure of Health Data for a Permitted Purpose as part of their job responsibilities. Network Participants and Member Affiliates shall establish and implement policies and procedures that:

i. Establish categories of Authorized Users;

ii. Define the purposes for which Authorized Users in those categories may access Health Data via the Network; and

iii. Define the types of Health Data that Authorized Users within such categories may access (e.g., demographic data only, clinical data).

b. The purposes for which an Authorized User may access Health Data via the Network and the types of information an Authorized User may access shall be based, at a minimum, on the Authorized User's job function and relationship to the patient.

REFERENCES: HIPAA Privacy Rule (45 C.F.R. § 164.502(b)).

Georgia ConnectedCare Services – Policy Number: GaHIN-1005

Policy Title: Accounting of Disclosures

PURPOSE: Consistent with the Network Facilitator's commitment to the principles of openness and transparency, accountability, and Patient access, this Policy is intended to ensure that all Network Participants and Member Affiliates develop and maintain processes through which Patients may obtain a record of Protected Health Information disclosures upon request. This Policy also describes Network Facilitator's responsibility as it relates to facilitating a Patient's ability to obtain information regarding the access and disclosure of their Protected Health Information through the Network.

SCOPE: This Policy applies to all Network Participants and Member Affiliates.

POLICY: Patients shall have the right to request and obtain an Accounting of Disclosures of their Health Data that is PHI made through the Network in accordance with Applicable Law, including HIPAA and HITECH.

The individual Network Participants (when applicable) and Member Affiliates, upon request, must provide a Patient with a record of the entities to which they have disclosed the Patient's Health Data consisting of PHI. Each Network Participant and Member Affiliate shall have a formal process through which Patients are able to request an Accounting of Disclosures from the Network Participant or Member Affiliate originating the PHI. Network Participants and Member Affiliates must comply with the requirements of 45 C.F.R. § 164.528 when providing an Accounting of Disclosures to a requesting Patient.

The Network Participants or Member Affiliates are the originators of Health Data containing PHI, and maintain the Designated Record Sets in which PHI resides. Likewise, Network Participants or Member Affiliates make the determination whether to disclose Health Data and log the disclosure if required to do so under the HIPAA Regulations. As such, the Network Participant or Member Affiliate whose Accounting of Disclosures is being sought by a Patient is the only organization that can logically evaluate and provide for a full Accounting of Disclosures of a Patient's Health Data that is PHI.

Accordingly, all requests for an Accounting of Disclosures made to the Network Facilitator will be forwarded to the appropriate Network Participants and Member Affiliates within 10 business days. The Network Facilitator shall not be obligated to nor will it directly respond to accounting requests received directly from a Patient. The Network Facilitator will, however, acknowledge receipt of the Patient's request for an accounting and notify the Patient in writing that their request has been sent to the Patient's Health Care Provider/Plan for processing and a response. The Network Participant or Member Affiliate will be solely responsible for preparing and delivering the requested accounting to the Patient in accordance with the HIPAA Regulations. To the extent required by law, the Network Facilitator will provide Network Participants with information in its possession necessary to enable Network Participants and/or Member Affiliates to timely respond to requests for an Accounting of Disclosures within the timeframe required by 45 C.F.R. § 164.528.

REFERENCES: HIPAA Privacy Rule (45 C.F.R. § 164.528).

Georgia ConnectedCare Services – Policy Number: GaHIN-1006

Policy Title: Workforce Members, Agents, and Contractors

PURPOSE: This Policy ensures legitimate use of Health Data, the proper implementation of Network Participants' and Member Affiliates' privacy practices, and the prompt identification of and undertaking of remedial action for privacy violations.

SCOPE: This Policy applies to all Network Participants and Member Affiliates.

POLICY:

1. **Access to System.** Each Network Participant and Member Affiliate shall allow access to the Network only by those Workforce members, agents, and contractors who have a legitimate and appropriate need to use the Network and/or release or obtain information through the Network. No Workforce member, agent, or contractor shall be provided with access to the Network without training on the Network Participant's or Member Affiliate's Policies and Network Facilitator's Policies.

2. **Discipline for Non-Compliance.** Each Network Participant and Member Affiliate shall implement procedures to hold Workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request Health Data except as permitted by the Network Participant's or Member Affiliate's policies and Network Facilitator's policies and that they comply with such policies.

3. **Reporting of Non-Compliance.** Each Network Participant and Member Affiliate shall have a mechanism for, and shall encourage, all Workforce members, agents, and contractors to report any non-compliance with policies to the Network Participant and/or Member Affiliate.

REFERENCES: 45 C.F.R. § 164.530.

Georgia ConnectedCare Services – Policy Number: GaHIN-1007
Policy Title: Opt-Out

PURPOSE: This purpose of this Policy is to describe how a Patient's decision to participate or not participate in the Network can be meaningfully exercised, and how that decision may be subsequently changed.

SCOPE: This Policy applies to all Network Participants and Member Affiliates.

POLICY: Patients will be offered a meaningful way to decide whether to participate or not participate in the Network by following an Opt-Out consent model. Under the Opt-Out consent model, Patients of a Network Participant or Member Affiliate will be automatically enrolled in the Network, and written HIPAA authorization shall not be required by the Patient to enroll in the Network. A Patient shall be deemed to have given his or her consent to participate until and unless the Patient affirmatively Opts-Out of the Network.

To ensure that Patients are able to make an informed choice, Network Participants and Member Affiliates that are Health Care Providers shall provide notice of the Patient's right to Opt Out of the Network. The notice may be included in the Health Care Provider's Notice of Privacy Practices or contained in a separate document. The notice should:

- explain the function of Health Information Exchange;
- describe the types of Health Data that may be, and may not be, exchanged via Health Information Exchange;
- identify the Permitted Purposes for disclosure of the Patient's Heath Data via Health Information Exchange;
- identify who and/or what entities will have access to the Patient's Health Data;
- describe the Patient's right to not share Health Data through Health Information Exchange or the right to Opt-Out;
- explain that a Network Participant or Member Affiliate is authorized to disclose the Patient's Health Data via Health Information Exchange unless and until the Patient elects to Opt Out by completing and submitting an Opt-Out form;
- state that an Opt-Out decision is in effect until the Patient notifies the Health Care Provider of their intent to participate in Health Information Exchange;
- describe the potential benefits and risks of participating in Health Information Exchange; and
- describe how the Patient's Health Data will be handled in the case of an Opt-Out.

Sample language for the notice may be provided by the Network Facilitator. In addition, the Network Facilitator will undertake other measures designed to inform Patients about the Network, including making educational materials available on the Network Facilitator's website.

If a Patient does not Opt-Out of Health Information Exchange, his or her Health Data will generally be disclosed in response to a specific request by a Network Participant or Member Affiliate for a Permitted Purpose, subject to Network Facilitator's policy on the exchange of Sensitive Health Information. (See Policy Number 1009, Restrictions of Sensitive Health Information).

A Patient may Opt Out of having their Health Data disclosed through the Network at any time, even after having already been enrolled in the Network. A Patient may revoke his or her decision to Opt Out at any time, provided that such revocation shall not preclude any Network Participant that has accessed Health Data via the Network prior to such revocation and incorporated such Health Data into its records from retaining such information in its records.

The Patient's choice to Opt Out of Health Information Exchange or revoke a prior decision to Opt Out of Health Information Exchange must be provided in writing through the Network Participant's or Member Affiliate's Patient consent process. All Network Participants and/or Member Affiliates must have a process for accepting written requests by Patients to Opt Out of having their Health Data disclosed

through the Network or to revoke their prior decision to Opt Out. Each Network Participant and/or Member Affiliate shall document and maintain, for a period of six years, documentation of all Patients' decisions to Opt Out or revoke a prior decision to Opt Out. Network Participants and/or Member Affiliates are responsible for sequestering the Health Data of Patients that have Opted Out and ensuring that it is not disclosed through the Network. If a Patient does Opt-Out, Network Participants and Member Affiliates will not be able to exchange his or her Health Data through the Network; however, Personal Demographic Information for the Patient will be submitted to the Network Facilitator for use in the Master Patient Index in accordance with the Master Patient Index Policy. (See Policy Number 1013, Master Patient Index).

Georgia ConnectedCare Services – Policy Number: GaHIN-1008
Policy Title: Permitted Purposes

PURPOSE: This Policy sets forth the Permitted Purposes for which Health Data may be disclosed through the Network from one Network Participant or Member Affiliate to another. While the HIPAA Regulations may permit use or disclosure for broader purposes, this Policy will set forth the uses and disclosures permitted for Network Facilitator's Directed Exchange and Query-Response services. The placement of appropriate limits upon the exchange of Health Data via the Network, through the definition of what constitutes a Permitted Purpose, will enhance Patient and provider confidence in the exchange process, and will minimize the potential for misuse or abuse of Health Data.

SCOPE: This Policy applies to all Network Participants and Member Affiliates.

POLICY: All disclosures of Health Data through the Network and the use of Health Data obtained through the Network shall be consistent with all Applicable Law and shall not be used for any unlawful or discriminatory purpose. If Applicable Law requires that certain documentation exist or that other conditions be met prior to using or disclosing Health Data that is PHI, the requesting Healthcare Provider shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing Healthcare Provider. Uses and disclosures of and requests for Health Data via the Network shall comply with all Network Facilitator's Policies. Each Network Participant and Member Affiliate shall refer to and comply with its own internal policies and procedures regarding disclosures of Health Data and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.

Network Participants' and/or Member Affiliates' requests, use, disclosures and transmittals of Health Data to and through the Network are also subject to the following limitations:

1. Health Care Provider. If Network Participant or Member Affiliate is a Health Care Provider, then Network Participant or Member Affiliate shall only request, receive, use and disclose Health Care Provider Health Data for a Patient, and solely for the purposes of Treatment of a Patient and Network Participant's or Member Affiliate's Payment and Health Care Operations related to a Patient or as otherwise legally authorized by a Patient.

2. Health Plan. If Network Participant or Member Affiliate is a Health Plan, then Network Participant or Member Affiliate shall only request, receive, use and disclose Health Plan Health Data for admission, discharge, and transfer purposes and such other purposes as approved in writing by a majority of the Network Participants.

3. HIO. If Network Participant is a HIO, then Network Participant shall only request, receive, use and disclose HIO Health Data, and solely for the purposes of Treatment, Payment, and Health Care Operations of Network Participant's Member Affiliates, or as otherwise legally authorized by a Patient, subject to and in accordance with Network Participant's contractual obligations with its participants.

4. State Agency. If Network Participant is a State Agency, then Network Participant shall only request, receive, use and disclose Health Data solely as authorized by Applicable Law or as legally authorized by a Patient.

Absent a Permitted Purpose, no exchange of Health Data will be authorized. Under no circumstances may Health Data be used or disclosed for any other purpose, including marketing or for discriminatory purposes.

Network Participants and Member Affiliates shall not request, receive, use, disclose or transmit Health Data for the purposes of selling or reselling or de-identified Health Data, comparing patient volumes, practice patterns, economic credentialing or tiering, underwriting, denial of coverage, otherwise analyzing

health outcomes or quality of care for the purposes of evaluating and adjusting health care provider reimbursement programs, or for any other purpose not expressly set forth in this Policy or the Member Agreement. Vendor shall not enter into any agreement with a Network Participant or Member Affiliate that does not contain limitations on such Network Participant's or Member Affiliate's right to request, receive, use, disclose or transmit Health Data that are identical to or substantially similar to those contained herein without the prior consent of all of the other Network Participants. Additional Permitted Purposes may be added to the definition of Permitted Purposes set forth in this Policy only by an amendment to the Member Agreement.

Georgia ConnectedCare Services – Policy Number: GaHIN-1009
Policy Title: Restrictions on Sensitive Health Information

PURPOSE: This policy defines how Network Participants and Member Affiliates may disclose Health Data that is subject to greater protection under federal and Georgia law ("Sensitive Health Information" or "SHI") through the Network.

SCOPE: This Policy applies to all Network Participants and Member Affiliates.

POLICY:

Federal and state laws impose heightened privacy and security requirements upon the disclosure of certain types of Health Data that may be considered particularly private or sensitive to a Patient. These laws require strict compliance, and Patient fears and concerns about their privacy must be given the utmost attention and respect. The heightened legal requirements for this type of Health Data that is PHI, which shall be generically referred to as Sensitive Health Information, cannot be adequately addressed by an Opt-Out policy. Depending upon the Permitted Purpose for which Sensitive Health Information is being sought, the law may require a Patient to specifically authorize in writing a disclosure of his or her Sensitive Health Information by signing a document that contains certain elements. Sensitive Health Information that requires the execution of a specific written authorization shall not be disclosed through the Network . SHI includes but is not limited to:

- substance abuse records;
- mental health and psychotherapy records;
- genetic testing information;
- HIV/AIDS information;
- developmental disability records.

Responsibility for restricting the transmission of SHI will reside with Network Participants and Member Affiliates. The sending Network Participant or Member Affiliate shall obtain an appropriate consent in accordance with Applicable Law from the Patient prior to disclosing or re-disclosing SHI through the Network. Network Participants and Member Affiliates shall meet all other obligations with respect to such SHI as required by Applicable Law.

REFERENCES: HIPAA Privacy Rule (45 C.F.R. §164.528); 42 C.F.R. Part 2; 45 C.F.R. § 164.508(a)(2); O.C.G.A. §§ 26-5-17, 33-54-3, 33-54-6, 43-39-16, 37-3-166, 37-4-125.

Georgia ConnectedCare Services – Policy Number: GaHIN-1010
Policy Title: Digital Certificate Policy

PURPOSE: This Policy governs the creation of Digital Certificates to identify Network Participants by name, address of place of business, or other disambiguating information and to enable the encrypted communication of information over the Network. Network Participants shall under the terms of the Member Agreement be obligated to verify identity of their Member Affiliates.

SCOPE: This Policy applies to all Network Participants in the Network Facilitator's Georgia ConnectedCare Services.

POLICY:

1. **Documentation Requirements:** Prior to the issuance of a Digital Certificate, the Vendor must obtain from the Applicant the following documentation, in compliance with the requirements of these Guidelines:

    a. Subscription Agreement;

    b. Member Agreement;

    c. Such additional documentation as the Vendor requires from the Applicant to satisfy its obligations under these Guidelines pursuant to the Member Agreement.

2. **Network Participant's Warranties and Representations:**

    a. Network Participant represents and warrants, during the period when the Digital Certificate is valid, that the information contained in the Digital Certificate is accurate;

    b. Network Participant warrants that it will not install and use the Digital Certificate until it has reviewed and verified the accuracy of the data contained therein;

    c. Network Participant warrants that it will take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Digital Certificate (and any associated access information or device, e.g. password);

    d. Network Participant warrants that it will install the Digital Certificate only on the server accessible at a Domain Name listed in the Digital Certificate, and to use the Digital Certificate solely in compliance with all Applicable Law, solely for authorized company business, and solely in accordance with the Subscriber Agreement;

    e. Network Participant warrants that it will promptly cease using a Digital Certificate, and promptly request the Vendor to revoke the Digital Certificate, in the event that there is any actual or suspected misuse or compromise of the Network Participant's Private Key associated with the Public Key listed in the Digital Certificate;

    f. Network Participant warrants that it will promptly cease all use of the Private Key corresponding to the Public Key listed in a Digital Certificate upon expiration or revocation of that Digital Certificate.

    g. Network Participant warrants that it will verify the identity of all its Member Affiliates.

3. **Time Cycle of Digital Certificate**

a. The identified time cycle for assigned Digital Certificates shall be one year from the date of issuance of the Digital Certificate.

b. A Digital Certificate may be renewed annually for up to three years. At the third year, the Network Participant must reapply for a new certificate.

c. The Vendor shall be responsible for managing the identified time cycle on assigned Digital Certificates.

d. During annual renewal of a Digital Certificate, the Network Participant shall validate the information contained within the Digital Certificate.

Georgia ConnectedCare Services – Policy Number: GaHIN-1011
Policy Title: Password Policy

PURPOSE: This Policy defines the requirements for passwords for those Network Participants and Member Affiliates who access the Network through the Georgia ConnectedCare Services web portal.

SCOPE: This Policy applies to Network Participants and Member Affiliates who access the Network through the Georgia ConnectedCare Services via the web portal only. Password requirements do not apply to Network Participant systems or information accessed through the Network Participant or Member Affiliate EHR.

POLICY: Network Participant and/or Member Affiliates must have unique passwords that meet, at a minimum, the following requirements:

- Minimum 8 characters
- Must have characters from at least 3 of the 4 character types
    - Upper-case letter
    - Lower-case letter
    - Number
    - Special character (!@#$%^&*)

Network Participants and/or Member Affiliates will be locked out after 3 failed log-in attempts. Network Participant and Member Affiliate accounts are automatically locked after 90 days of inactivity. The Network Participants and Member Affiliates must contact the Help Desk to reset their password in the event of lockout or to reactivate their account. Passwords must be changed every 90 days.

An Authorized User shall not share his or her password with any other individual, and must change his or her password periodically to ensure ongoing security. An Authorized User will be reminded of this change to his or her password automatically by Network Facilitator upon log-in.

*NOTE: All configuration standards are maintained in the Network Facilitator's configuration master document.

Georgia ConnectedCare Services – Policy Number: GaHIN-1012
Policy Title: Patient Record Matching

PURPOSE: The purpose of this Policy is to define the criteria used for matching patient records in response to a Network Participant or Member Affiliate query through Georgia ConnectedCare Services.

SCOPE: This policy applies to the Vendor, Network Participants, and Member Affiliates.

POLICY: Patient records are located and matched only in response to an authorized Network Participant or Member Affiliate request.

Portal Search: Records are matched based on the information entered to the search screen by the Member Affiliate. Searches submitted through the portal must include the Patient's last name. In addition, searches must include one of the following fields:

- Date of Birth
- Social Security Number, Medicaid Number or Insurance ID Number

The accuracy of the match is dependent on the amount of information entered by the Network Participant or Member Affiliate. When less information is entered, the number of possible matches increases and will be presented to the Network Participant or Member Affiliate for selection of the appropriate record.

Master Patient Index (MPI) query: Queries to the Network will be based on MPI matches. The minimum patient data needed for effective Patient linking is Date of Birth, First name, Last name and Middle initial. Social security number and/or Medicaid recipient number are strongly recommended and highly desirable. Other data such as full street address and phone number can be added to increase matching rates.

Georgia ConnectedCare Services – Policy Number: GaHIN-1013
Policy Title: Master Patient Index

PURPOSE: The purpose of this Policy is to describe the establishment and operation of a Master Patient Index by the Network. The purpose of the Master Patient Index is to serve as the permanent record of a Patient's decision to either participate in the Network or to Opt Out.

SCOPE: This policy applies to the Network, Network Participants and Member Affiliates.

POLICY: Under the Patient Opt-Out Policy (Policy Number 1007), Patients are offered a meaningful way to express their decision to either participate or not participate in the Network. A Patient who does not want his or her Health Data to be disclosed to other Network Participants or Member Affiliates may Opt-Out of Health Information Exchange. A Patient shall be deemed to have given his or her consent to participate in Health Information Exchange until and unless the Patient affirmatively Opts-Out.

In order for the Network Facilitator to comply with each Patient's decision, it must establish a database to permanently record this decision. This database will require the inclusion of a subset of Protected Health Information—Personal Demographic Information—from each Patient of a Network Participant or Member Affiliate, even if the decision was made to Opt-Out. This is necessary to minimize the possibility of improperly matching a Patient who has Opted-Out with another Patient who is participating.

The Master Patient Index will include only Personal Demographic Information – Patient names and other non-clinical details used to identify the Patient (date of birth, address, telephone number, driver's license number, etc.). The Master Patient Index will be promptly updated in accordance with any change in the Patient's decision to participate or not participate in Health Information Exchange.

As Personal Demographic Information is a category of PHI, the Network Facilitator will ensure that it maintains the privacy and security of the Personal Demographic Information it electronically stores in the Master Patient Index in accordance with Applicable Law, and will ensure that such Personal Demographic Information will not be shared with third parties outside the Network who are not Network Participants or Member Affiliates.

Georgia ConnectedCare Services – Policy Number: GaHIN-1014
Policy Title: Data for Research and Analytics

PURPOSE: The purpose of this Policy is to define the role of Network Facilitator in the exchange of data for research and analytics.

SCOPE: This Policy applies to all Network Participants, Member Affiliates, and Network Facilitator's Georgia ConnectedCare Services vendor.

POLICY: Network Facilitator and its network vendor do not own or steward any Health Data or any aggregated de-identified health information that can be used for health care analytics or research. All requests for such data are solely between Network Participants and/or Member Affiliates in accordance with Applicable Law.

Georgia ConnectedCare Services – Policy Number: GaHIN-1015
Policy Title: Breach Notification

PURPOSE: This Policy sets forth minimum standards that the Network Facilitator, Vendor, Network Participants and Member Affiliates shall follow in the event of Breach of Unsecured PHI. The purpose of this policy is to establish a notification process in compliance with the HITECH Act and the HIPAA Regulations for a Breach of Unsecured PHI.

SCOPE: This Policy applies to the Network Facilitator, Vendor, Network Participants, and Member Affiliates.

POLICY: Federal and state laws protect Patients from the improper acquisition, access, use or disclosure of their PHI by unauthorized persons and entities. In its performance of the functions of a Health Information Exchange, Vendor may receive and exchange a Patient's PHI from one Network Participant to another. Vendor's electronic receipt and transport of Health Data consisting of PHI qualifies it under the law as a Business Associate to its Network Participants. This status of a Business Associate places obligations upon the Vendor if a Patient's PHI should ever be the subject of a Breach when residing in or passing through the Network.

"Breach" shall be defined in accordance with 45 C.F.R. § 164.402, as may be amended, to be the unauthorized acquisition, access, use or disclosure of Protected Health Information in a manner not permitted under Subpart E of 45 C.F.R. § 164.402, when such information is exchanged via the Network. The notification process contemplated by Applicable Law applies only if the Breach involves Unsecured PHI. Unsecured PHI means that the PHI has not been rendered unusable, unreadable, or indecipherable by unauthorized individuals or entities through the use of encryption or other federally-approved technology.

Vendor, Network Participants and Member Affiliates shall develop a Breach plan as part of their policies and procedures. Network Participants shall require their Member Affiliates to notify the Network Participant in the event a Member Affiliate determines, in accordance with its internal policies and procedures for investigating and confirming a Breach, that there has been a Breach of Health Data consisting of Unsecured PHI that is exchanged via the Network. Network Participant will notify the Vendor of a Breach of Unsecured PHI by Network Participant or its Member Affiliate in the most expedient time possible and without unreasonable delay, but no later than twenty-four (24) hours after confirming, following a reasonable time for investigation in accordance with the Network Participant's or Member Affiliate's internal policies and procedures, that a Breach has occurred. Notification shall comply with the HIPAA Regulations, HITECH and Applicable Law. Network Participants shall provide the Vendor with appropriate points of contact for Breach notification and shall promptly notify Vendor if those points of contact change.

Vendor will notify Network Facilitator and each Network Participant that Vendor believes is reasonably likely to have been impacted of a Breach of Unsecured PHI by Vendor in the most expedient time possible and without unreasonable delay, but no later than twenty-four (24) hours after confirming, following a reasonable time for investigation in accordance with the Vendor's internal policies and procedures, that a Breach has occurred. Notification shall comply with the HIPAA Regulations, HITECH and Applicable Law. Vendor shall provide Network Facilitator and Network Participants with appropriate points of contact for Breach notification and shall promptly notify Network Facilitator and Network Participants if those points of contact change.

In the event of a Breach by a Network Participant or a Member Affiliate, the Vendor and Network Facilitator, in cooperation with each other, may conduct an investigation of such Breach, determine the extent of the Breach, determine corrective actions, and may apply such sanctions on Network Participants as a result of such Breach as permitted by the applicable Member Agreement. Network Participants and Member Affiliates shall cooperate in any investigation conducted by the Network Facilitator, Vendor, state, or federal government authorities.

In the event of a Breach by Vendor, the Network Participants reasonably likely to have been impacted such Breach and Network Facilitator, in cooperation with each other, may conduct an investigation of such Breach, determine the extent of the Breach, determine corrective actions, and may exercise all rights and remedies provided to such parties under their respective agreements with Vendor. Vendor shall cooperate in any investigation conducted by the Network Facilitator, Network Participant, state, or federal government authorities and as reasonably requested by Network Participant in order for Network Participant and its Member Affiliates, as applicable, to satisfy their respective obligations under the breach notification requirements of the HIPAA Regulations and other Applicable Law.

When Vendor, a Network Participant or a Member Affiliate becomes aware of a suspected or actual Breach, Vendor, such Network Participant or such Member Affiliate, as applicable, shall comply with its internal policies and procedures for investigating and confirming a Breach, which should include, if commercially practicable, following Network Facilitator's Breach Response Procedures, as applicable, to the extent such procedures do not conflict with the internal policies and procedures of such Vendor, Network Participant or Member Affiliate.

Notification of a Breach of Unsecured PHI should include sufficient information for the recipient to understand the nature of the Breach; provided, however, that the notification shall not include any PHI. Such notification should include, to the extent available at the time of the notification, the following information:

- Brief description of the Breach;
- Description of the roles of the people involved in the Breach (e.g., employees, Member Affiliates, service providers, unauthorized persons, etc.);
- A description of the type of PHI subject to the Breach;
- Network Participants and their respective Member Affiliates likely impacted by the Breach;
- Number of Patients or records impacted/estimated to be impacted by the Breach;
- Actions taken by notifying party to mitigate the Breach;
- Current status of the Breach (i.e. under investigation or resolved); and
- Corrective action taken and steps planned to be taken to prevent any similar or additional Breach.

The Vendor or Network Facilitator may, at its sole discretion, notify non-impacted Network Participants of any Breach. If Vendor or Network Facilitator determines that (i) the other Network Participants that have not been notified of the Breach would benefit from a summary of the notification; or (ii) a summary of the notification to the other Network Participants would enhance the security of the Network, then Vendor or Network Facilitator may provide, in a timely manner, a summary to such Network Participants that does not identify any of the Network Participants, Member Affiliates, or Patients involved in the Breach, unless such identification was previously approved by such Network Participant, Member Affiliate, or Patient.

Vendor, each Network Participant and/or each Member Affiliate shall establish appropriate sanctions that shall apply to their Authorized Users in the event of a Breach and shall apply such sanctions. Such sanctions may include, but shall not be limited to, temporarily restricting an Authorized User's access to the Network, termination by a Network Participant of a Member Affiliate's access to the Network, or such other remedies as Vendor, Network Participant or Member Affiliate may deem reasonably necessary in accordance with its internal risk analysis.

The Network Facilitator participates in the eHealth Exchange, or the nationwide Health Information Exchange, and must comply with the Breach notification procedures outlined in DURSA. Therefore, when a Breach occurs, the Network Participant or Member Affiliate must determine whether the Breach also constitutes a DURSA Breach. A DURSA Breach is defined as:

> the unauthorized acquisition, access, disclosure, or use of Message Content while sending, requesting, receiving, responding to, or otherwise exchanging or disclosing such Message Content via the eHealth Exchange. "Breach" does not include the following: (1) any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Network Participant or Member Affiliate if: (a) such acquisition, access, disclosure or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Network Participant or Member Affiliate; and (b) such Message Content is not further acquired, accessed, disclosed, or used by such employee or individual; or (2) any acquisition, access, disclosure or use of information contained in or available through the Network Participant's systems where such acquisition, access, disclosure or use was not directly related to sending, requesting, receiving, responding to, or otherwise exchanging or disclosing Message Content via the eHealth Exchange.

Message Content includes, but is not limited to, Protected Health Information, de-identified data, individually identifiable information, pseudonymized data, metadata, schema and Digital Credentials. In other words, if a Breach (or suspected Breach) occurs *while* the Network Participant or Member Affiliate is sending, requesting, receiving, or accessing an electronic transmission of Health Data through the eHealth Exchange, the Breach must be reported in accordance with the procedures outlined below. But if the Breach was from the Network Participant's or Member Affiliate's electronic health record or electronic records system and did not occur while (i.e., at the same time) the Network Participant or the Member Affiliate was using the eHealth Exchange, the Breach is considered to be not directly related to the DURSA and should not be reported as a DURSA Breach.

When the Network Facilitator discovers information that leads it to reasonably believe that a DURSA Breach may have occurred, the Network Facilitator must comply with the following notification procedures:

- Within one (1) hour of discovery of information that leads the Network Facilitator to reasonably believe that a DURSA Breach may have occurred, the Network Facilitator is required to notify the eHealth Exchange Coordinating Committee and eHealth Exchange participants that may have been affected;

- As soon as reasonably practicable, but no later than 24 hours after confirmation that a DURSA Breach has occurred, the Network Facilitator is required to provide written notice to the eHealth Exchange Coordinating Committee, as well as any eHealth Exchange participants who have likely been impacted by the DURSA Breach;

- The Network Facilitator must supplement information provided about a DURSA Breach and provide reasonable assistance to the eHealth Exchange Coordinating Committee and other eHealth Exchange participants in the investigation of a DURSA Breach.

In order to facilitate the Network Facilitator's compliance with the notification requirements of the DURSA, Vendor, Network Participants and Member Affiliates must take the following actions upon discovery of information that leads Vendor, Network Participant or Member Affiliate to reasonably believe that a DURSA Breach may have occurred:

- Notify Network Facilitator *immediately* after discovering information that leads Vendor or a Network Participant to reasonably believe that a DURSA Breach may have occurred, but in no event later than twenty-four (24) hours after discovery.

  - Vendor, Network Participants and Member Affiliates should use caution before relaying details of the suspected DURSA Breach via e-mail, and are urged to send such notification through a secure means. The notification should include a brief description of the information that led the notifying party to reasonably believe that a DURSA Breach may have occurred, and list the eHealth Exchange participants that may have been impacted by the DURSA Breach.

- Notify Network Facilitator *immediately* after confirming that a DURSA Breach has occurred, but in no event later than twenty-four (24) hours after such confirmation. Notification must be in the form of a written report to Network Facilitator. This report shall not contain any PHI. Notifying parties are urged to send the report through a secure means, where appropriate and possible. The report should contain, to the extent available at the time of the report, the following information:

  - One or two sentence description of the DURSA Breach;

  - Description of the roles of the people involved in the DURSA Breach (e.g., employees of Network Participant or Member Affiliate, service providers, unauthorized persons, etc.);

  - The type of Message Content breached;

  - eHealth Exchange Participants likely impacted by the DURSA Breach;

  - Number of Patients or records impacted/estimated to be impacted by the DURSA Breach;

  - Actions taken by the notifying party to mitigate the DURSA Breach;

  - Current status of the DURSA Breach; and

  - Corrective action taken and steps planned to be taken to prevent a similar DURSA Breach.

Vendor, Network Participant or Member Affiliate, as applicable, shall supplement the information contained in a report as it becomes available, and shall reasonably cooperate with Network Facilitator in the investigation of a Breach or a DURSA Breach. The obligations of Vendor, Network Participant and Member Affiliate contained in this Policy, and in the DURSA, are in addition to and do not supersede Vendor's or such Network Participant's or Member Affiliate's obligations under relevant security incident, breach notification or confidentiality provisions of Applicable Law. Compliance with this Policy shall not relieve the Vendor, Network Facilitator, a Network Participant, or a Member Affiliate of any other security incident or breach reporting requirements under Applicable Law including, but not limited to, those related to consumers and the breach of computerized personal information.

REFERENCES: HIPAA Regulations (45 C.F.R. § 164.402); eHealth Exchange Data Use and Reciprocal Support Agreement.

Georgia ConnectedCare Services – Policy Number: GaHIN-1016
Policy Title: eHealth Exchange

PURPOSE: This policy is intended to ensure that all Network Participants and Member Affiliates comply with the requirements of the eHealth Exchange, as set forth in the Data Use and Reciprocal Support Agreement (DURSA).

SCOPE: This Policy applies to all Network Participants and Member Affiliates.

POLICY: Network Facilitator participates in the eHealth Exchange, or the nationwide health information network. As a participant in the eHealth Exchange, Network Facilitator must cause its Network Participants and Member Affiliates to comply with certain requirements of the DURSA. When exchanging Health Data via the eHealth Exchange, Network Participants and Member Affiliate shall, at a minimum:

1. Comply with all Applicable Law;
2. Reasonably cooperate with Network Facilitator on all issues related to the DURSA and use of the eHealth Exchange;
3. Request, retrieve, and exchange Health Data via the eHealth Exchange only for a Permitted Purpose as defined in these Policies (which is more restrictive than the DURSA definition);
4. Use data received through the eHealth Exchange in accordance with Applicable Law and the Network Participant's or Member Affiliate's data retention policies;
5. Report suspected and confirmed DURSA Breaches to Network Facilitator as set forth in the Breach Notification Policy; and
6. Refrain from disclosing any passwords, certificates, or any other security measures issued to the Network Participant or Member Affiliate that enables connectivity to the eHealth Exchange.

REFERENCES: eHealth Exchange Data Use and Reciprocal Support Agreement (DURSA).