

HealtheConnections Privacy and Security Policy and Procedures Handbook ("Policies and Procedures")

May 29, 2026

Introduction

HealtheConnections, Inc. ("HealtheConnections"), a New York Not-for-Profit corporation, manages a Regional Health Information Organization (RHIO), also known as a Qualified Entity (QE) to facilitate health information sharing and aggregation for treatment, operations, public health and research related purposes in a manner that complies with all applicable laws and regulations, including without limitation, those protecting the privacy and security of health information. This document entitled "HealtheConnections Privacy and Security Policy and Procedures Handbook" (the "Policies and Procedures") sets forth the Policies and Procedures governing participation in HealtheConnections. This guidance ensures secure health information exchange through the Statewide Health Information Network for New York (SHIN-NY) by addressing the full range of privacy and security policies for an interoperable health information exchange, including authorization, authentication, consent, access, audit, breach, and patient engagement policies. All of the policies and procedures that are within this handbook have been developed from the Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State, per 10 NYCRR 300.3(b)(1). These policies and procedures were developed by the New York State Department of Health ("NYS DOH") in compliance with state and federal laws, along with other key stakeholders, through the Statewide Collaboration Process ("SCP"). It is the policy of HealtheConnections that each Authorized User be trained on and certified as understanding and accepting the policies and procedures in this handbook, and that Participants support HealtheConnections in ensuring their Authorized Users' compliance in accessing patient information through the health information exchange.

Relationship to Terms and Conditions

This document along with the Participation Agreement (to include the Statewide Common Participation Agreement), Business Associate Agreement, and Terms and Conditions apply to the operation of HealtheConnections, the provision of services, and the relationship among HealtheConnections and its Participants with respect thereto. Capitalized terms not specifically defined herein or in Appendix A hereto, shall have the meaning set forth in the Terms and Conditions. Policies and Procedures Review and Amendment Process These Policies and Procedures were developed by HealtheConnections. HealtheConnections will be responsible for reviewing and updating these policies and procedures and making appropriate changes to comply with changes in the law, including the relevant standards and implementation requirements of HIPAA, ARRA, the State of New York, and New York State Department of Health through the SCP. Changes will be made in accordance with the provisions contained in Section 16.1(f) of the Terms & Conditions and will be distributed to the RHIO Administrator. The current version of these Policies and Procedures is available on our Resource Center webpage.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

Table of Contents

1 Consent Policy ____ 5
1.1 Requirement to Obtain Affirmative Consent (prior to accessing patient records). ____ 5
1.2 Exceptions to Affirmative Consent. ____ 5
1.3 Form of Patient Consent. ____ 7
1.4 Sensitive Health Information. ____ 8
1.5 Special Provisions Relating to Minors. ____ 9
1.6 De-Identified Data. ____ 9
1.7 Research. ____ 10
1.8 Transmittals to Non-Participants. ____ 11
1.9 Other Policies and Procedures Related to Consent. ____ 12
1.10 Patient Consent Transition Rules. ____ 14
1.11 Waivers During a Public Health Emergency. ____ 14
2 Authorization Policy ____ 15
2.1 Role-Based Access. ____ 15
3 Authentication Policy ____ 17
3.1 Obligation to Ensure Authentication of Identity of Authorized User Prior to Access. ____ 17
3.2 Authentication Requirements. ____ 17
3.3 Compliance with Policies Resulting from Statewide Risk Analysis. ____ 17
3.4 Option to Rely on Statewide Authentication Service. ____ 17
3.5 Authentication of Certified Applications and Downstream Users. ____ 17
4 Access ____ 18
4.1 HealtheConnections Access Policy and Procedure. ____ 18
4.2 Authorized Purposes. ____ 18
4.3 Failed Access Attempts. ____ 18
4.4 Periods of Inactivity. ____ 18
4.5 Access Limited to Minimum Necessary Information. ____ 18
4.6 Record Locator Service and Other Comparable Directories. ____ 19
4.7 Training. ____ 19
4.8 Termination of Access and Other Sanctions. ____ 19
4.9 Access by Certified Applications. ____ 19
4.10 Participation Agreements. ____ 19
5 Patient Education, Engagement and Access ____ 20
5.1 Patient Education Resources. ____ 20

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

5.2 Patient Access to SHIN-NY Data. 20
5.3 Patient Direction to Patient Apps and Other Third Parties. 20
5.4 Information About Minors. 20
5.5 Patient Input and Participation. 20
5.6 Requests to Correct Erroneous Information. 20
6 Audit 21
6.1 Audit Logs. 21
6.2 Periodic Audits. 21
6.3 Participant Access to Audit Logs. 21
6.4 Patient Access to Audit Log Information. 21
6.5 Public Availability of Audits. 21
6.6 Correction of Erroneous Data. 22
6.7 Weekly Audit Reports by Organ Procurement Organizations. 22
6.8 Additional Requirements Related to Auditing of Public Health Access. 22
7 Breach 23
7.1 Obligation of Participants to Report Actual or Suspected Breaches. 23
7.2 Responsibilities of HealtheConnections. 23
8 Compliance 24
8.1 Covered Entities. 24
8.2 Non-Covered Entitles. 24
8.3 Community Based Organizations Not Subject to HIPAA. 24
9 Sanctions 25
9.1 HealtheConnections Sanction Policy & Procedure. 25
9.2 Factors Considered in Sanction Determination. 25
9.3 Sanctions That May Be Applied. 25
10 Cybersecurity 26
10.1 Certification. 26
10.2 Role of Statewide CISO. 26
10.3 Cybersecurity Policy and Procedures (CSPP). 26
10.4 CSPP Content. 26
10.5 CSPP Review. 27
10.6 Cybersecurity Insurance. 27
Appendix A: Definitions 28

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

1 Consent Policy

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding consent. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

1.1 Requirement to Obtain Affirmative Consent (prior to accessing patient records).

HealtheConnections will provide each participant with customized consent form(s) during the on-boarding process; HealtheConnections-provided form(s) must be used by the participant to collect consent from patients. Consent forms signed by patients must be maintained for 6 years. Per SHIN-NY regulations, consents must be signed (paper or electronic), not verbal.

Access is only allowed if the patient selects the option to allow Access (e.g., "I GIVE CONSENT").
The consent value on the form must match the value entered in the system. If consent is entered in the system incorrectly, please email Support@healtheconnections.org to correct the consent, or contact Support by phone at 315-671-2241 x5. Additional information regarding consent is available under "more references" on our Resource Center webpage.

Should the Participant desire to integrate the paper consent form in their electronic health records system, the following requirements apply: 1) the electronic version must exactly match the verbiage of the paper form; 2) the electronic version form must be tested by HealtheConnections; this testing will include a review of the output for all consent options; 3) the Participant must have the ability to print a copy of the form for the patient; 4) the Participant must provide a printed copy to the patient upon patient request. Participants shall contact HealtheConnections Support prior to implementing an electronic Consent form, so that HealtheConnections can conduct the appropriate review and testing. Such Participants shall email Support@healtheconnections.org or contact Support by phone at 315-671-2241 x5 to initiate this process.

1.2 Exceptions to Affirmative Consent.

Disclosures of Protected Health Information without Affirmative Consent shall comply with applicable federal, state and local laws and regulations, including 42 C.F.R. Part 2. Protected Health Information subject to 42 C.F.R. Part 2 shall not be Disclosed without Affirmative Consent unless 42 C.F.R. Part 2 specifically allows for such Disclosure.

1.2.1 One-to-One Exchanges.

HealtheConnections will provide an agreement to be signed by both parties engaging in a One-to-One Exchange as it is defined in Appendix A. Interested Participants shall contact Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5 to obtain this agreement.

1.2.2 Public Health Reporting and Access.

Public Health Participants and/or their users may receive reports and/or have Access to certain dashboards for the purposes allowed under, and in accordance with, SHIN-NY regulations Section 1.2.2 and subsections. Users who work in a Public Health Agency will be assigned to a Public Health Role (credentials, see Appendix A) that allows Access to patient record look-up without consent for purposes authorized under SHIN-NY regulations Section 1.2.2 and subsections; this includes purposes such as disease monitoring and investigations to reduce morbidity and mortality. Public Health users must record the reason for accessing the PHI, corresponding with those permitted purposes. If the Public Health Agency also operates

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

a clinic, users are *not* allowed to access PHI using their Public Health Role for clinical Level 1 Uses - (Treatment, Care Management, Quality Improvement); instead, users will be issued a separate a separate role for clinical access and must collect consent in accordance with Section 1.1 of SHIN-NY regulations and Section 1.1 of these Policies and Procedures, above. Users who need separate role based access will need to fill out separate Authorized User requests, available on our Resource Center webpage, or can use this direct link: New User Request Form

1.2.3 Disaster Tracking.

In the case of a declared disaster, HealtheConnections will make a patient locator report (see Record Locator Service in Appendix A) available to Disaster Relief Agencies' authorized users for this purpose.

1.2.4 Emergency Disclosures of Protected Health Information When Treating a Patient with an Emergency Condition or "Breaking the Glass.".

As permitted by HIPAA and SHIN-NY regulations, HealtheConnections does not require Affirmative Consent to access the records of a patient that is experiencing a life-threatening emergency that meets all the requirements defined under SHIN-NY regulations Section 1.2.4 (referred to as Break the Glass). Users who are not Practitioners or Emergency Medical Technicians shall record the name of the Practitioner who authorized their use of Break the Glass. This functionality is only available to certain organizations and their users, refer to Break the Glass FAQs for more information. HealtheConnections will monitor all Break the Glass accesses by the Participant or Daily audits are required for Break the Glass access. Users who improperly use Break the Glass and/or Participants that fail to complete their audits will be subject to sanctions, as described in SHIN-NY regulations Section 4.8.

1.2.5 Converting Data.

As a Business Associate of our Data Suppliers, HealtheConnections may receive PHI without patient consent. Access to data uploaded to HealtheConnections is not Disclosed until Affirmative Consent is obtained, except as otherwise permitted in these Policies and Procedures.

1.2.6 Access for Operational Use.

HealtheConnections and its vendors may Access or receive PHI without Affirmative Consent for operations and other purposes, in accordance with SHIN-NY regulations Section 1.2.6.

1.2.7 De-Identified Data.

HealtheConnections may disclose De-Identified Data without Affirmative Consent as permitted in Section 1.6.

1.2.8 Organ Procurement Organization (OPO) Access.

OPO Participants may Access PHI without Affirmative Consent solely for the purposes of facilitating organ, eye, or tissue donations or transplants, even if a Community Wide Deny is in place for the patient.

1.2.9 Patient Care Alerts.

HealtheConnections provides Patient Care Alerts to Participants following the requirements established in SHIN-NY regulations Section 1.2.9. New Authorized Users who would like to receive Patient Care Alerts can add this functionality by completing a New User Request Form. Existing Authorized Users who would like

to receive Patient Care Alerts can add this functionality by completing a User Account Modification & Termination Form. Additional resources regarding Patient Care Alerts can be found under "additional resources" on our Resource Center webpage.

1.2.10 Disclosures to Payer Organizations for Quality Measures.

HealtheConnections requires Payer Organizations to execute a Payer Addendum to their Participation Agreement prior to making Disclosures to such Participants as permitted under SHIN-NY regulations Section 1.2.10. Interested Payer Organizations shall contact Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5 to obtain this agreement.

1.2.11 Death Notifications.

HealtheConnections may disclose limited information about the death of a patient to a treating Participant or a Payer Organization, as described in SHIN-NY regulations Section 1.2.11.

1.2.12 Death Investigators.

Medical Examiners and Death Investigators may Access PHI without Affirmative Consent, provided that the requirements stipulated in SHIN-NY regulations Section 1.2.12 are met.

1.2.13 Telehealth.

HealtheConnections and their Participants are required to follow SHIN-NY regulations Section1.2.13, with respect to collecting consent during a Telehealth visit. Further guidance on this exception to written consent is available on our Resource Center webpage: Written Consent Exceptions.

1.2.14 Utilization Review Requirements.

SHIN-NY regulations Section 1.2.14 allows disclosure for the purpose of Utilization Review; however, the NYS DOH authorized Level 1 Uses Model Consent Form (available in SHIN-NY regulations Attachment A-1 and A-2) does not allow for uses of PHI that will affect payment of patient medical bills. For this reason, HealtheConnections does not allow Participants to access PHI for this purpose unless the Participant obtains an Affirmative Consent on a Level 2 Consent form provided by HealtheConnections; see also Section 1.1 of these Policies and Procedures.

1.3 Form of Patient Consent.

HealtheConnections does not allow Alternative Consent as permitted under SHIN-NY regulations Section 1.3 and subsections. The only Approved Consent will be the form provided to the Participant and as described in Section 1.1 of these Policies and Procedures.

1.3.1 Level 1 Uses.

The only Approved Consent will be the form(s) provided to the Participant as described in Section 1.1 of these Policies and Procedures. HealtheConnections does not approve Alternative Consent forms for Level 1 Uses. HealtheConnections supports the following Level 1 Uses: Treatment, Quality Improvement, Care Management, and Insurance Coverage Reviews, as those uses are defined in SHIN-NY regulations and Appendix A. HealtheConnections does not support the use of a Level 1 Consent form for the purpose of Utilization Review, refer also to Section 1.2.14 of these Policies and Procedures. Payer Organizations shall use a Level 2 consent form for Utilization Review.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

1.3.2 Level 2 Uses.

The only Approved Consent will be the form(s) provided to the Participant as described in Section 1.1 of these Policies and Procedures. HealtheConnections does not approve Alternative Consent forms for Level 2 Uses. HealtheConnections supports the following Level 2 Uses: Payer Payment (including Utilization Review) and Research.

1.3.3 Separate Consents.

HealtheConnections follows SHIN-NY regulations Section 1.3.3. Separate Level 1 and Level 2 consents will be provided to the Participant by HealtheConnections for Participants that require such forms for Level 1 and Level 2 Uses as described in Sections 1.3.1 and 1.3.2, respectively, of these Policies and Procedures.

1.3.4 Level 2 Consents Related to Marketing.

HealtheConnections does not support Level 2 Consents Related to Marketing

1.3.5 Naming a QE and Recognition of Consents.

A consent form that is signed by a patient permitting Disclosure (an Affirmative Consent) on a state approved form that meets the requirements of SHIN-NY regulations Section 1.3.1 shall permit disclosure of such patient's PHI by a QE, even if such QE is not named on the Level 1 Consent, provided that all the requirements of SHIN-NY regulations Section 1.3.5 are met.

1.3.6 Statewide Consent and Statewide Consent Management.

NYSDOH made the decision to suspend implementation of the statewide consent form. Work on advancing the Statewide Consent Registry (SCR) will continue. You can read the full memo here: NYeC April 2026 memo.

1.3.7 Expiration at Death.

Affirmative Consent shall expire upon an individual's death. However, HealtheConnections may disclose the individuals PHI in accordance with the terms of Affirmative Consent, until HealtheConnections has determined (based on records from Participants or government agencies) that the individual has died.

1.4 Sensitive Health Information.

1.4.1 General.

When a patient signs an Affirmative Consent their Sensitive Health Information will be available to Participants identified on the consent form.

1.4.2 Withing Holding Sensitive Information.

Participants may, but are not required to, offer patients the option of preventing certain sensitive health information from being shared with HealtheConnections; in this case, the Participant may exercise this option by not contributing such data to HealtheConnections. HealtheConnections does not post an alert indicating that data has been withheld from the record.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

1.4.3 Re-Disclosure Warning.

HealtheConnections posts a Re-Disclosure warning notice that meets all requirements of SHIN-NY regulations Section 1.4.3 and subsections. This Re-Disclosure warning notice is available on the patient look-up portal and included on Transmittals.

1.5 Special Provisions Relating to Minors.

Refer to HealtheConnections Minor Consented Services Override Access FAQs for additional information regarding Minor Consented Services, which requires a separate consent form and specific procedures for Access to PHI about minors that includes Minor Consented Services.

1.5.1 Consent to Access Minors' PHI.

Participants may access or receive PHI about minors (other than Minor Consented Services) based on Affirmative Consent that is executed by the minor's Personal Representative. Participants may access or receive PHI about Minor Consented Services based on Affirmative Consent that is executed by the minor.

1.5.2 Permitted Access to Minors' PHI.

Federal and/or state law or regulation requires the minor's authorization for certain Disclosures (e.g., Minor Consented Services), in which case a Participant may not Access or receive such information without the minor's Affirmative Consent.

1.5.3 Disclosure of Minors' PHI.

HealtheConnections and Participants shall not disclose information regarding Minor Consented Services to the minor's Personal Representative without the minor's written consent.

1.6 De-Identified Data.

1.6.1 General Considerations.

HealtheConnections may disclose de-identified data without Affirmative Consent if a data use agreement is entered into with the recipient in accordance with SHIN-NY regulations Section 1.6.3. If it is determined that the data will be used to assist in marketing activities that would not comply with the HIPAA privacy rule, or if the proposed use for the data is not keeping with the mission of the SHIN-NY, HealtheConnections shall not disclose such data. A data use agreement is not required if HealtheConnections is only Transmitting patient counts as described in SHIN-NY regulations Section 1.6.1.

1.6.2 De-identification Standards.

Both HealtheConnections and their Participants must comply with standards for the deidentification of data set forth in 45 C.F.R. § 164.514.

1.6.3 Data Use Agreement.

HealtheConnections' Data Use Agreement language complies with the language required under SHIN-NY regulations Section 1.6.3. Interested Participants shall contact Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5 to obtain this agreement.

443 North Franklin St., Suite 001
Syracuse, NY 13204

1.6.4 Data Suppliers.

Following SHIN-NY regulations Section 1.6.4, any Disclosures will comply with the terms that are set in the Business Associate Agreement that is signed by both HealtheConnections and the Data Supplier that is the source of the De-Identified Data.

1.7 Research.

HealtheConnections' policy and procedure regarding Research:

A. Research Request form: Once HeC receives a Research request, the researcher will be asked to complete the HeC Research Request form. The form will be used to evaluate the project and will be provided to the designated approver (see 1.7.C, below). Researchers may contact Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5 to obtain this form.

B. Review and approval required: Research requests must be reviewed and approved by the designated approver (see 1.7.C, below). Researchers can expect HealtheConnections' review and approval process to require a minimum of four weeks to complete. If a researcher seeks to obtain information from multiple QEs for purposes of Research, then the QEs and the researcher shall comply with SHIN-NY regulations Section 1.7.5.

C. Designated approver: Research involving PHI shall be approved by an Institutional Review Board. Research involving a Limited Data Set or De-Identified Data shall be approved by HealtheConnections' QE Research Review Committee. The foregoing notwithstanding, if Research involving a Limited Data Set or De-Identified Data has been approved by an Institutional Review Board, the Reseach may be approved by HealtheConnections' internal Data Review Committee in lieu of HealtheConnections' QE Research Review Committee.

D. Review of requests: The review of such requests will consider, at a minimum: whether the request complies with applicable laws and regulations, including but not limited to, HIPAA and SHIN-NY regulations; whether the request aligns with HealtheConnections mission; whether such request is permitted under agreements with Data Suppliers; whether there are sufficient resources to undertake the project; whether the request includes mental health clinical information governed by Section 33.13 of the Mental Hygiene Law; and, whether such request requires patient consent.

E. Approval criteria: Requests shall not be approved unless the review determines that the request complies with applicable laws and regulations; aligns with HealtheConnections mission; is permitted under agreements with Data Suppliers; there are sufficient resources to undertake the project; the Disclosure does not include any mental health clinical information governed by Section 33.13 of the Mental Hygiene Law, unless the recipient of the Disclosure is a facility as defined in the Mental Hygiene Law; and, the researcher will collect Affirmative consent unless the Disclosure is permitted without Affirmative Consent and all requirements for Disclosure without Affirmative Consent are met.

F. Requirements for approved requests: HealtheConnections and Researcher shall execute a Data Use Agreement (DUA) when required by SHIN-NY regulations and/or the HIPAA Privacy Rule.

G. DUA requirements, if applicable: Approved requests for De-Identified Data must execute a DUA that meets the requirements for those of De-Identified Data set forth in SHIN-NY regulations Section 1.6.3. Approved requests for Limited Data Sets must execute a DUA in accordance with the HIPAA Privacy Rule. HealtheConnections' may execute a DUA provided by the Researcher or, alternatively, may provide a DUA form to the Researcher for execution.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

1.7.1 Research Involving De-Identified Data.

As disclosed to Participants in the Terms & Conditions Section 3.b, HealtheConnections may create De-Identified Data sets using PHI received from Data Suppliers provided HealtheConnections complies with 45 C.F.R. § 164.514 and the SHIN-NY SOPs with respect to the creation of such data set and the use and disclosure of such De-Identified Data.

1.7.2 Research Involving a Limited Data Set.

HealtheConnections and Participants shall follow HealtheConnections' policy and procedure regarding Research as defined in Section 1.7 of these Policies and Procedures.

1.7.3 Research Involving Protected Health Information.

HealtheConnections and Participants shall follow HealtheConnections' policy and procedure regarding Research as defined in Section 1.7 of these Policies and Procedures. The foregoing notwithstanding, Affirmative Consent shall not be required for a QE to Disclose the name and other identifying information of an individual who may qualify for a Research study to a Participant that has a treating relationship with such individual so that the Participant may contact the individual to determine the individual's willingness to participate in such study, provided that all of the requirements stipulated under SHIN-NY regulations Section 1.7.3 are met. Once those patients have been identified, HealtheConnections will provide the researchers with: a list of patients who qualify for the study; a Level 2 Consent which must be completed by the patient to allow Access to their PHI for research purposes, refer to Section 1.1 of these Policies and Procedures regarding form of consent. It is the researcher's responsibility to gather the Level 2 Consent forms from the patients; Affirmative Consent must be obtained by the researchers and provided to HealtheConnections prior to Accessing PHI.

1.7.4 Other Requirements.

In accordance with SHIN-NY regulations Section 1.7.4, a Participant may not opt out of having its PHI de-identified or converted into a limited data set and used for research purposes when such request complies with SHIN-NY regulations Section 1.7.1, 1.7.2, or 1.7.5, if applicable.

1.7.5 Research Involving Multiple QEs.

If a researcher seeks to obtain information from multiple QEs for purposes of Research, via sPRL or otherwise, then the QEs and the researcher shall comply with SHIN-NY regulations Section 1.7.5. Refer also to HealtheConnections' policy and procedure regarding Research as defined in Section 1.7 of these Policies and Procedures.

1.8 Transmittals to Non-Participants.

1.8.1 Transmittals to Business Associates.

If a Participant requests that HealtheConnections Transmit PHI to a Business Associate, HealtheConnections shall provide such Participant with an agreement (HealtheConnections Authorization Agreement For Disclosure of Data to Participant's Vendor) that meets all the requirements of SHIN-NY regulations Section 1.8.1. This agreement shall be executed by such Participant and HealtheConnections to permit the Transmittal. Participants may contact Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5 to obtain this agreement.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

1.8.2 Transmittals to Other Non-Participants.

HealtheConnections may Transmit a patient's Protected Health Information from the QE (or any other QE that has agreed to such Transmittal) to a health care provider or other entity that is not a Participant or a Business Associate of a Participant only if all of the conditions stipulated in SHIN-NY regulations Section 1.8.2 are met.

1.9 Other Policies and Procedures Related to Consent.

1.9.1 Affiliated Practitioners.

An Affirmative Consent that applies to a Participant shall apply to an Affiliated Practitioner of the Participant provided that the requirements stipulated in SHIN-NY regulations Section 1.9.1 are met.

1.9.2 Authorized Users.

An Affirmative Consent obtained by a Participant shall permit Authorized Users of the Participant to Access information covered by the Affirmative Consent in accordance with SHIN-NY regulations Sections 2 and 4.

1.9.3 Multi-Participant Consent.

Multi-Participant consent forms may be provided to Participant(s), following the requirements stipulated in these Policies and Procedures Section 1.1, provided that the requirements of SHIN-NY regulations Section 1.9.3 are met. Participants may contact Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5 to request a multi-participant consent form.

1.9.4 Consent Obtained by HealtheConnections.

Under SHIN-NY regulations Section 1.9.4., HealtheConnections may obtain, on behalf of their Participants, consents that meet the requirements of SHIN-NY regulations Section 1.

1.9.5 Electronic Signatures.

Electronically signed consents must meet the requirements of SHIN-NY regulations Section 1.9.5. Electronic consent forms must be approved by HealtheConnections, refer to Section 1.1 in these Policies and Procedures.

1.9.6 Denial of Consent.

In accordance SHIN-NY regulations Section 1.9.6, a patient's decision not to sign a consent shall not be construed as a "denial of consent" under SHIN-NY regulations Section 1.2.4(a)(iii). HealtheConnections gives patients options to deny consent to all Participants by the execution of a Community Wide Deny. The Community Wide Deny form may be provided to patients by HealtheConnections or Participants. Patients and/or Participants may obtain this form by contacting Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5. Participants who receive a Community Wide Deny executed by a patient shall send this form to HealtheConnections via one of the following methods: a) Secure Message to support@hiemail.healtheconnections.org); b) encrypted email to Support@healtheconnections.org; c) fax to 315-407-0053. More information on a Community Wide Deny is available on our Resource Center website in Patient Resources.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

1.9.7 Durability.

Consents must be expired following the requirements of SHIN-NY regulations Section 1.9.7. Participants shall contact HealtheConnections to expire consents via one of the following methods: a) Secure Message to support@hiemail.healtheconnections.org); b) encrypted email to Support@healtheconnections.org; c) fax to 315-407-0053; d) phone to 315-671-2241 x 5.

1.9.8 Revocability.

Patients may change their consent at any time by completing a new patient consent form. Participants shall accommodate a patient's request to complete a new consent form.

1.9.9 Notification of a QE's Data Suppliers.

HealtheConnections maintains a list of all the Data Suppliers on our website in accordance with SHIN-NY regulations Section 1.9.9.

1.9.10 Business Associate Agreements with Data Suppliers.

HealtheConnections executes a standard Business Associate Agreement (BAA) with all Data Suppliers in accordance with SHIN-NY regulations Section 1.9.10, and may disclose PHI in accordance with the BAA. HealtheConnections is a collaborative health exchange; for this reason, HealtheConnections does not permit modifications to our standard BAA unless required by law or regulation.

1.9.11 Disclosure to HealtheConnections' Vendors.

HealtheConnections may may Disclose Protected Health Information to vendors that assist in carrying out the QE's authorized activities provided that the requirements of SHIN-NY regulations Section 1.9.11 are met.

1.9.12 Compliance with Existing Law.

HealtheConnections and their Participants comply with all federal, state and local laws and regulations and shall meet all documentation and/or conditions stipulated under SHIN-NY regulations. Participants shall provide evidence thereof to HealtheConnections in accordance with SHIN-NY regulations Section 1.9.12, upon request.

1.9.13 Restrictions on Disclosures to Payer Organizations.

Upon a Provider Organization's receipt of a patient's request that Protected Health Information created by the Provider Organization not be Disclosed to a Payer Organization, such Provider Organization shall immediately notify HealtheConnections of the restriction; HealtheConnections will apply the appropriate denial of consent to the Payer Organization for the patient. Upon receipt of a subsequent Affirmative Consent executed by said patient for said Payer Organization, the recipient of such Affirmative Consent shall inform the patient that the affirmative consent will revoke the previous denial of consent. If the patient agrees to the revocation of the prior denial, the recipient of the Affirmative Consent shall inform HealtheConnections that the patient has agreed to the revocation; HealtheConnections will then expire the denial.

1.9.14 Policies for Governing Disclosures to Government Agencies for Health Oversight.

HealtheConnections policies for governing Disclosures to Government Agencies for Health Oversight: HealtheConnections will review such requests, except for requests that fall under SHIN-NY regulations Section 1.2, using the following policy and procedure: 1) With respect to access to PHI for health oversight

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

purposes such as Medicaid audits, professional licensing reviews, and fraud and abuse investigations, HealtheConnections, unless required by law, will not disclose information to health oversight agencies, without affirmative consent. Participants will not be notified of such disclosures; 2) Any request for disclosure received from a government agency for health oversight will be submitted through HealtheConnections' Service Delivery Process for completion. HealtheConnections shall validate the authenticity of any such request prior to disclosing any PHI to such agency.

1.9.15 Indication of Medical Orders of Life Sustaining Treatment (MOLST).

Under SHIN-NY regulations Section 1.9.15 HealtheConnections may note whether a patient has signed a MOLST without Affirmative Consent through its Record Locator Service.

1.9.16 Consent for Access by ACOs and IPAs.

HealtheConnections and its Participants shall follow SHIN-NY regulations Section 1.9.16 with respect to Affirmative Consent authorizing Access by an ACO or IPA.

1.10 Patient Consent Transition Rules.

HealtheConnections and their Participants may continue to use existing Affirmative Consents after the Consent Implementation Date if the existing consent is approved by NYS DOH under SHIN-NY regulations Section 1.3.

1.11 Waivers During a Public Health Emergency.

NYS DOH may waive provisions of SHIN-NY regulations Section 1 and other provisions of SHIN-NY regulations during a public health emergency under Section 319 of the Public Health Services Act in accordance with SHIN-NY regulations Section 1.11.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

2 Authorization Policy

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding authorization. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

2.1 Role-Based Access.

2.1.1 HealtheConnections Policies and Procedures for Role-Based Access.

HealtheConnections has established and implemented policies and procedures for Role-Based Access, refer to Sections 2.1.2 - 2.1.6, below.

2.1.2 Relationship of Role-Based Access to the Authorized User's Job Function.

As part of the Authorized User application, the individual requesting such Access must verify that the level of Access requested is consistent with their job function; further, the individual Authorizing such Access (normally the RHIO Administrator) must attest to the fact that the purposes for which an Authorized User may Access information via the SHIN-NY and the types of information an Authorized User may Access are based on the Authorized User's job function and relationship to the patient.

2.1.3 Role-Based Access Standards.

HealtheConnections has established the following categories of Authorized Users, which define the types of PHI such Authorized User may Access. Access to PHI is limited in accordance with the category indicated on an approved Authorized User form.

A. BTG - a (i) Practitioner; (ii) Authorized User acting under the direction of a Practitioner; or (iii) Emergency Medical Technician who, under the provisions of SHIN-NY regulations Section 1.2.4, has temporary rights to Access Protected Health Information for a specific patient.
B. Practitioner with access to clinical and non-clinical information to look-up a patient and enter/verify a consent value, or for purposes stipulated on the Affirmative Consent executed by the patient authorizing the Disclosure, or other activities authorized under SHIN-NY regulations.
C. Non-practitioner with access to clinical and non-clinical information to look-up a patient and enter/verify a consent value, or for purposes stipulated on the Affirmative Consent executed by the patient authorizing the Disclosure, or other activities authorized under SHIN-NY regulations.
D. Non-practitioner with access to non-clinical information to look-up a patient and enter/verify a consent value, or for purposes stipulated on the Affirmative Consent executed by the patient authorizing the Disclosure, or other activities authorized under SHIN-NY regulations.
E. QE administrator with access to non-clinical information for purposes permitted under SHIN-NY regulations Section 1 or other activities authorized under SHIN-NY regulations.
F. QE administrators with Access to clinical information in order to engage in public health reporting in accordance with SHIN-NY regulations Section 1.2.2, or other activities authorized under SHIN-NY regulations.
G. QE or Participant administrators with Access to clinical and non-clinical information for purposes of system maintenance and testing, troubleshooting and similar operational and technical support

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

purposes, in accordance with SHIN-NY regulations Section 1.2.5, Section 1.2.6, or other activities authorized under SHIN-NY regulations.

H. Public Health users who bypass consent, with Access to clinical and non-clinical information for purposes permitted under SHIN-NY regulations Section 1.2.2., or other activities authorized under SHIN-NY regulations.

I. Organ Procurement users who bypass consent, with Access to clinical and non-clinical information for purposes permitted under SHIN-NY regulations Section 1.2.8., or other activities authorized under SHIN-NY regulations.

J. Death Investigator users who bypass consent, with Access to clinical and non-clinical information for purposes permitted under SHIN-NY regulations Section 1.2.12., or other activities authorized under SHIN-NY regulations.

2.1.4 Participant Designated Main Contact.

The main contact of the Participant shall be designated as the RHIO Administrator. The RHIO Administrator will be authorized to Access information via the SHIN-NY and to ensure those individuals are assigned to the appropriate categories as listed above. The RHIO Administrator shall also approve/deny Authorized User forms for their organization. Additional resources are available under the heading "rhio administrator" on our Resource Center webpage.

2.1.5 Individuals whose Access to Data may Bypass or Enable Circumvention of Activity Logging.

HealtheConnections subjects these Authorized Users to heightened scrutiny both in hiring and in ongoing auditing and monitoring of their activities, in compliance with SHIN-NY regulations Section 2.1.5.

2.1.6 Requirements for Certified Applications to Access PHI Through the SHIN-NY.

Certified Applications must be approved by HealtheConnections through a security review process that ensures that such applications satisfy all encryption and other security standards incorporated into the SHIN-NY Policy Standards through the SCP.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

3 Authentication Policy

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding the authentication process. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

3.1 Obligation to Ensure Authentication of Identity of Authorized User Prior to Access.

A HealtheConnections representative will meet with a designated Indvidual (Participant's RHIO Administrator) prior to implementing any QE processes. Once the Participant is fully onboarded, the RHIO Administrator will authenticate the identity of any Authorized User who is requesting access to the HIE from that organization. HealtheConnections conducts annual identity proofing audits to verify compliance with this provision; Participants shall cooperate with such audit requests, or may face sanctions for failure to do so, in accordance with Section 4.8 of these Policies and Procedures.

3.2 Authentication Requirements.

HealtheConnections software has been configured to meet or exceed the requirements set forth in SHIN-NY regulations Section 3.2. Authorized users must enable multifactor authentication; for additional information, refer to Multi-Factor Authentication FAQs.

3.3 Compliance with Policies Resulting from Statewide Risk Analysis.

HealtheConnections and its Participants acknowledge that a statewide risk analysis may identify additional or revised authentication policies and procedures, which shall be developed and approved through the SCP before adoption.

3.4 Option to Rely on Statewide Authentication Service.

New York State has not developed statewide services for the authentication of Authorized Users.

3.5 Authentication of Certified Applications and Downstream Users.

HealtheConnections' security review of Certified Applications (refer to Section 2.1.6 of these Policies and Procedures) shall ensure such applications comply with the authentication requirements set forth in SHIN-NY regulations Section 3.5.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

4 Access

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding accessing the HIE. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

4.1 HealtheConnections Access Policy and Procedure.

A. Each Authorized User shall have a unique username, whether provisioned though HealtheConnections or a Certified Application.
B. Each Authorized User shall be authenticated in accordance with the provisions of Section 3.
C. Group or temporary usernames shall be prohibited.
D. Authorized Users shall be required to change their passwords in accordance with the NIST SP 800-63 guidelines, as may be revised periodically.
E. Authorized Users shall be prohibited from sharing their usernames, passwords or other authentication tools (e.g., tokens), with others and from using the usernames, passwords or other authentication tools of others.
F. Authorized Users shall be provisioned using our online webform application: New User Request Form. Privileges shall be modified or revoked using our User Account Modification & Termination Form. Additional information and resources are available here: Resource Center
    a. These forms must be approved by the respective Participant's RHIO Administrator, their delegate, or HealtheConnections staff.
G. Authorized Users are permitted Access only where such Access is consistent with these Policies and Procedures.

4.2 Authorized Purposes.

Access to PHI via the SHIN-NY only for purposes consistent with a patient's Affirmative Consent or an exception set forth in SHIN-NY regulations Section 1.2.

4.3 Failed Access Attempts.

HealtheConnections software is configured to disable Authorized Users with consecutive failed Access attempts in compliance with SHIN-NY regulations Section 4.3.

4.4 Periods of Inactivity.

HealtheConnections software is configured to log out Authorized Users after 15 minutes of inactivity in compliance with SHIN-NY regulations Section 4.4.

4.5 Access Limited to Minimum Necessary Information.

Participants and their Authorized Users shall ensure that reasonable efforts are made, except in the case of Access for Treatment, to limit the information Accessed via the SHIN-NY to the minimum amount necessary to accomplish the intended purpose for which the information is Accessed. in compliance with SHIN-NY regulations Section 4.5.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

4.6 Record Locator Service and Other Comparable Directories.

HealtheConnections software is configured to minimize the amount of demographic information reasonably necessary to enable Authorized Users to successfully identify a patient through its Record Locator System and reduce the risk of unauthorized incidental Disclosures of Protected Health Information during the process of identifying a patient and locating a patient's medical records, in compliance with SHIN-NY regulations Section 4.6.

4.7 Training.

HealtheConnections requires each Authorized User to undergo training in compliance with SHIN-NY regulations Section 4.7. Refer to Resource Center for more information and training materials. Authorized Users and the Participant's RHIO Administrator are required to sign an attestation that such Authorized User has received training and will comply with these Policies and Procedures; this attestation is part of the Authorized User application, available here: New User Request Form. Approved New User Request Forms shall be retained by Participants for at least six years. Authorized Users shall complete refresher training to maintain their credentials; HealtheConnections software is configured to disable access if refresher training is not completed by the due date. HealtheConnections' trainings focus on SHIN-NY specific requirements, including managing consent. Evidence of training shall be maintained for at least six years.

4.8 Termination of Access and Other Sanctions.

HealtheConnections policies and procedures for termination of Access and other sanctions:

A. Upon termination of a Participant's Participation Agreement, HealtheConnections Operations Support will terminate access to ALL Authorized Users affiliated with that Participant within one business day.
B. Upon termination of employment or affiliation of an Authorized User with a Participant, the Participant must notify HealtheConnections Support, in writing, as promptly as reasonably practicable (i.e., within one business day). HealtheConnections Operations Support will terminate access for the named Authorized User within one business day of notification.
C. HealtheConnections Operations Support will terminate access for an Authorized User within one business day of notification of a Breach, or suspected Breach, by such Authorized User.
D. HealtheConnections Operations Support may apply sanctions, up to and including termination of Access as a result of other non-compliance of these Policies and Procedures by a Participant and/or an Authorized User.
E. Refer also to Section 9 of these Policies and Procedures for further information on Sanctions.

4.9 Access by Certified Applications.

HealtheConnections and its Participants that access PHI via a Certified Application shall meet all the requirements set forth in SHIN-NY regulations Section 4.9.

4.10 Participation Agreements.

HealtheConnections and its Participants shall execute a Participation Agreement and collect consent as required by SHIN-NY regulations Section 4.10.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

5 Patient Education, Engagement and Access

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding patient education, engagement and access. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

5.1 Patient Education Resources.

HealtheConnections provides patient education and resources on our Resource Center webpage in Patient Resources, and also provides patient education materials to Participants on our Resource Center webpage, in accordance with SHIN-NY regulations Section 5.1 and its subsections.

5.2 Patient Access to SHIN-NY Data.

HealtheConnections provides several methods allowing patients to Access SHIN-NY data on our Resource Center webpage in Patient Resources, and abides by all requirements stipulated in SHIN-NY regulations Section 5.2 and its subsections. In addition, patients may contact Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5 for additional information or to request a paper copy of our Record Request Form. HealtheConnections shall only facilitate such Access after confirming the identity of the patient or the patient's Personal Representative through adequate identity proofing procedures.

5.3 Patient Direction to Patient Apps and Other Third Parties.

HealtheConnections provides methods for patients to direct their data to third parties on our Resource Center webpage in Patient Resources, and abides by all requirements stipulated in SHIN-NY regulations Section 5.3 and its subsections. In addition, patients may contact Support via email Support@healtheconnections.org or by phone at 315-671-2241 x5 for additional information or to request a connection to a Patient App. HealtheConnections shall only Disclose patient data after confirming the identity of the patient or the patient's Personal Representative through adequate identity proofing procedures.

5.4 Information About Minors.

HealtheConnections allows Access to information about Minors only as permitted in SHIN-NY regulations Section 5.4.

5.5 Patient Input and Participation.

HealtheConnections encourages patient input by the operation of our Contact Us functionality on our website, including on the Resource Center webpage in Patient Resources, and by inclusion of people from various backgrounds on our Board of Directors.

5.6 Requests to Correct Erroneous Information.

HealtheConnections directs patients to the appropriate Participant(s) to resolve an inquiry or dispute over the accuracy or integrity of their PHI, and to have erroneous information corrected or to have a dispute documented if their request to revise data is denied. HealtheConnections and its Participants shall follow the guidance provided in SHIN-NY regulations Section 5.6 when handling of such requests.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

6 Audit

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding audit practices. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

6.1 Audit Logs.

HealtheConnections' Audit Logs are maintained and produced through the HIE software and are maintained for at least six years from the date of access. Audit logs are configured to meet all requirements set forth in SHIN-NY regulations Section 6.1.1 through 6.1.5.

6.2 Periodic Audits.

Participants shall audit their Affirmative Consents, Authorized Users and Accesses as required by SHIN-NY regulations Section 6.2. Each Participant shall designate individual(s) responsible for completing any requested audits; this person is referred to as the Audit Report Recipient. Resources and the procedure for audits are available under the heading "audit report recipients" on our Resource Center webpage. HealtheConnections will select a statistically significant sample of Participants to be audited and ensure the content and cadence of audits meets or exceeds the requirements set for in SHIN-NY regulations Section 6.2.1 through 6.2.6. HealtheConnections will send a notification to Participants when audits are due. Participants are required to complete their audits within four weeks; failure to complete an audit in a timely manner may result in Sanctions (refer to Section 9 of these Policies and Procedures).

6.3 Participant Access to Audit Logs.

HealtheConnections shall provide its Participant Access to Audit Logs within 10 days, upon request, following the requirements set forth in SHIN-NY regulations Section 6.3. The Audit Logs provided may be limited to data dated back 6 years from the date of the request.

6.4 Patient Access to Audit Log Information.

HealtheConnections and its Participants shall provide Patients with Access to Audit Logs within 10 days, upon request, and shall comply with the requirements for patient Access to information set forth in SHIN-NY regulations Section 6.4 and subsections. A Participant RHIO Administrator shall, upon request, assist with the fulfillment of such patient request and shall: 1) verify the identity of any Patient who presents at their office with a HealtheConnections' Patient Audit Log Request Form; 2) sign as a witness in the designated field; 3) submit the signed form to HealtheConnections in an expedient and secure manner via one of the following mechanisms: a) fax 315- 407-0053; b) Secure Message to support@hiemail.healtheconnections.org; c) encrypted email to Support@healtheconnections.org. Information on how patients can request a copy of the audit logs, and the Patient Audit Log Request Form are available on our Resource Center website. The Audit Logs provided may be limited to data dated back 6 years from the date of the request.

6.5 Public Availability of Audits.

Results of audits of Participants are available on our Resource Center website in Patient Resources, and are updated within 30 days of completion.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

6.6 Correction of Erroneous Data.

HealtheConnections shall investigate, log, resolve, and notify Participants of, issues related to erroneous data that resulted from HealtheConnections data aggregation and exchange activities, in accordance with SHIN-NY regulations Section 6.6.

6.7 Weekly Audit Reports by Organ Procurement Organizations.

Organ Procurement Organizations are required to complete their audits on a weekly basis (see Section 6.2 of these Policies and Procedures for additional audit policies and procedures).

6.8 Additional Requirements Related to Auditing of Public Health Access.

HealtheConnections shall provide Public Health Participants with regular audit reports, and Public Health Participants shall review these reports in accordance with SHIN-NY regulations Section 6.8. These audits shall be completed on a monthly basis (see Section 6.2 of these Policies and Procedures for additional audit policies and procedures).

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

7 Breach

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding breaches. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

7.1 Obligation of Participants to Report Actual or Suspected Breaches.

Under SHIN-NY regulations Section 7.1, Participants shall notify HealtheConnections in writing, in the most expedient time possible and without unreasonable delay, if they become aware of any actual or suspected Breach of Unsecured Protected Health Information Accessed or Transmitted via the SHIN-NY.

7.2 Responsibilities of HealtheConnections.

HealtheConnections has developed a Breach plan which will be made available to Participants upon request. Additional information regarding the reporting of privacy and/or security events/incidents is available under the heading "more references" on our Resource Center webpage.

Upon receipt of notice of an actual or suspected Breach:

A. HealtheConnections will activate its Breach Plan, which meets the requirements set forth in SHIN-NY regulations Section 7.2.1 and 7.2.2.
B. HealtheConnections will provide the Participant who reported the Breach with an Information Gathering Form; such Participant shall complete and return the form in the most expedient time possible and without unreasonable delay.
C. Participant who reported the Breach shall attend meetings as necessary to collect any additional information regarding the Breach.
D. For a confirmed Breach:
    a. The responsible Participant shall notify the patient(s) and any applicable regulatory agencies as required by and in accordance with applicable federal, state and local laws and regulations, including but not limited to HITECH.
        i. For the avoidance of doubt, with respect to a Breach that is caused by an Authorized User who Accessed or Disclosed PHI in violation of HIPAA, the responsible Participant is the Participant who approved such Authorized User.
    b. HealtheConnections will send notice to the patient's data sources, within 60 days of the reported breach.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

8 Compliance

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding compliance. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

8.1 Covered Entities.

Each Participant that is a Covered Entity must comply with the HIPAA Privacy & Security Rule.

8.2 Non-Covered Entitles.

Each Participant that is not a Covered Entity, other than a public health authority or a Health Oversight Agency, must comply with the HIPAA Privacy & Security Rule as set forth in SHIN-NY regulations Section 8.2.

8.3 Community Based Organizations Not Subject to HIPAA.

HealtheConnections follows SHIN-NY regulations Section 8.3 and will conduct due diligence in regard to any Community Based Organization that is not a Covered Entity that is seeking to become a Participant. HealtheConnections may reject the entity if the organization does not have sufficient security protocols. Any Participant that is a Community Based Organization that is not a Covered Entity is subject to the requirements of SHIN-NY regulations Section 8.2 and subsections, and SHIN-NY regulations Section 8.3 and subsections. Note that, with respect to such Community Based Organization: Access to and Transmittal of PHI is limited and must take into account the nature of the Community-Based Organization. Re-Disclosure of PHI received via the SHIN-NY by such Community Based Organization may only be made to the patient or the patient's Personal Representative and/or another Participant for purposes of Treatment or Care Management.

Additional resources are available to Community Based organizations here: Community Health

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

9 Sanctions

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding sanctions. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

9.1 HealtheConnections Sanction Policy & Procedure.

HealtheConnections has developed the following sanction policy and procedure, in accordance with SHIN-NY regulations Section 9 and subsections:

A. Participants and Public Health Agencies shall inform all their Authorized Users about HealtheConnections' sanctions policies. Authorized Users may access these Policies and Procedures which include our sanction policy and procedure, under the heading "Policy Information" on our Resource Center webpage.
B. HealtheConnections shall apply sanctions for noncompliance, taking into account the factors listed under SHIN-NY regulations Section 9.2, and whether the non-compliance was related to an individual Authorized User, or to a Participant as a whole.
    a. For a recurring and/or uncorrected matter of non-compliance that has resulted in a sanction, the sanction applied may escalate, as illustrated by the following example:
        i. If a Participant does not complete their audit in a timely manner, the first sanction applied may be retraining; if the retraining is not effective and the audit remains incomplete, the sanction may escalate to include the suspension of the Participant's Authorized Users.
    b. Participants shall, upon request, provide information to HealtheConnections to assist in the identification of relevant factors.
C. Sanctions shall include, but are not limited to, the sanctions listed under SHIN-NY regulations Section 9.3. HealtheConnections may apply other reasonable sanctions that are not specifically identified in SHIN-NY regulations Section 9.3, such as requiring additional monitoring/auditing of an Authorized User, as may be appropriate to the situation. HealtheConnections may consult Participant and the "ISC Sanctions Table" when making the determination of the appropriate sanction.
D. HealtheConnections will make its best efforts to inform the Authorized Users and/or Participant of the sanction being applied, but such notification may occur after the sanction has been applied.

9.2 Factors Considered in Sanction Determination.

HealtheConnections considers all relevant factors when determining the sanction to be applied, in accordance with SHIN-NY regulations Section 9.2.

9.3 Sanctions That May Be Applied.

HealtheConnections may apply any sanctions specifically included in SHIN-NY regulations Section 9.3. In addition, HealtheConnections may apply other reasonable sanctions, as may be appropriate to the situation and as described in HealtheConnections sanction policy and procedure detailed in Section 9.1, above, of these Policies and Procedures.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

10 Cybersecurity

HealtheConnections, its Participants and their users are required to follow Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1) (SHIN-NY regulations) regarding cybersecurity. HealtheConnections' specific implementation requirements are below. The reference number below corresponds with the section number of SHIN-NY regulations.

10.1 Certification.

HealtheConnections shall be certified by the NYS DOH-approved certification body as set forth in SHIN-NY regulations Section 10.1.

10.2 Role of Statewide CISO.

HealtheConnections shall collaborate with the Statewide CISO as set forth in SHIN-NY regulations Section 10.2.

10.3 Cybersecurity Policy and Procedures (CSPP).

HealtheConnections maintains Cybersecurity Policy and Procedures (CSPP) as set forth in SHIN-NY regulations Section 10.3. HealtheConnections CSPP is confidential; however, HealtheConnections will cooperate with Participants and the SHIN-NY Enterprise to provide information regarding HealtheConnections' Cybersecurity program, such as by providing evidence of the completed certification referenced above in Section 10.1 of these Policies and Procedures.

10.4 CSPP Content.

HealtheConnections' CSPP shall include policies and procedures that are consistent with the requirements of the NYS DOH-approved certification body and address the areas identified in SHIN-NY regulations Section 10.4.1 through in SHIN-NY regulations Section 10.4.7. HealtheConnections' specific requirements regarding certificate issuance, trust stores, and related exceptions are as follows:

i. HealtheConnections shall issue public key certificates under an organization-operated Certificate Authority (CA), or obtain public key certificates from a third-party trusted Certificate Authority. Third-party trusted CAs shall be limited to publicly trusted CAs whose root certificates are included in a widely recognized trust program, such as the CA Browser Forum or equivalent.
ii. Only trust anchors included in a widely recognized trust program, such as the CA Browser Forum or equivalent, shall be included in trust stores or certificate stores managed by HealtheConnections.
iii. Third-party private Certificate Authorities not operated by HealtheConnections are prohibited from issuing certificates for TLS or mutual TLS (mTLS) authentication. Certificates presented for TLS or mTLS shall chain to a trust anchor that is either (a) operated by HealtheConnections, or (b) a publicly trusted CA included in a widely recognized trust program, such as the CA Browser Forum or equivalent.
iv. Private CA roots or intermediates not under HealtheConnections' control shall not be installed into any HealtheConnections -managed trust store for the purpose of authenticating TLS or mTLS connections.
v. No exceptions to sections (iii) or (iv) shall be permitted unless expressly approved in writing by the Chief Executive Officer. Any such exception shall be considered temporary, shall not exceed 60 days from the date of approval. All exceptions shall be reviewed every 60 days, documented in the HealtheConnections risk register, including the business justification, scope, and expiration date. Upon expiration, any non-conforming certificates shall be revoked.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

10.5 CSPP Review.

HealtheConnections shall conduct an annual review of its CSPP as directed by NYS DOH and prescribed by the statewide CISO.

10.6 Cybersecurity Insurance.

HealtheConnections shall maintain cybersecurity insurance that meets or exceeds the level specified in the QEPA.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

Appendix A: Definitions

Access means the ability of an Authorized User or Certified Application to view Protected Health Information on a QE's electronic health information system following the Authorized User's or Certified Application's logging on to such QE.

Accountable Care Organization (ACO) means an organization of clinically integrated health care providers certified by the Commissioner of Health under N.Y. Public Health Law Article 29- E.

Affiliated Practitioner means (i) a Practitioner employed by or under contract to a Provider Organization to render health care services to the Provider Organization's patients; (ii) a Practitioner on a Provider Organization's formal medical staff or (iii) a Practitioner providing services to a Provider Organization's patients pursuant to a cross-coverage or on-call arrangement.

Affirmative Consent means the consent of a patient obtained through the patient's execution of (i) a Level 1 Consent; (ii) a Level 2 Consent; (iii) an Alternative Consent; or (iv) a consent that may be relied upon under the Patient Consent Transition Rules set forth in Section 1.10.

Alternative Consent means a consent form approved under Section 1.3 as an alternative to a Level 1 Consent or a Level 2 Consent.

Approved Consent means an Affirmative Consent other than a consent relied upon by a Participant under the Patient Consent Transition Rules set forth in Section 1.10.

Audit Log means an electronic record of the Disclosure of information via the SHIN-NY, such as, for example, queries made by Authorized Users, type of information Disclosed, information flows between the QE and Participants, and date and time markers for those activities.

Audit Report Recipient* will receive access to HeC audit reports through the HealtheConnections user portal. The reports are then used to complete the required audits (annual, BTG, etc.)

Authenticator Assurance Level 2 (AAL2) means the authentication categorization set forth in NIST SP 800-63 which provides high confidence that the individual seeking access controls authenticator(s) bound to the Authorized User's account. Under AAL2, proof of possession and control of two distinct authentication factors are required through secure authentication protocol(s).

Authorized User means an individual who has been authorized by a Participant or a QE to Access patient information via the SHIN-NY in accordance with these Policies and Procedures.

Breach means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the Protected Health Information. An acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Participant or QE can demonstrate that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the Protected Health Information or to whom the disclosure was made; (iii) whether the Protected Health Information was actually acquired or viewed; and (iv) the extent to which the risk to the Protected Health Information has been mitigated. Breach excludes: (i) any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of a QE or Participant, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; (ii) any inadvertent

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

disclosure by a person who is authorized to access Protected Health Information at a QE or Participant to another person authorized to access Protected Health Information at the same QE or Participant, or organized health care arrangement in which a Participant participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or (iii) a disclosure of Protected Health Information where a QE or Participant has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Break the Glass (BTG) means the ability of an Authorized User to Access a patient's Protected Health Information without obtaining an Affirmative Consent in accordance with the provisions of Section 1.2.4.

Business Associate Agreement means a written signed agreement meeting the HIPAA requirements of 45 C.F.R. § 164.504(e).

Care Management means (i) assisting a patient in obtaining appropriate medical care, (ii) improving the quality of health care services provided to a patient, (iii) coordinating the provision of multiple health care services to a patient, (iv) supporting a patient in following a plan of medical care, or (v) assisting a patient in obtaining social services or providing social services to a patient.

CARIN Alliance means the multi-sector collaborative that seeks to advance consumer-directed exchange of health information and which has developed a list of recommended Patient Apps via its "My Health Application" website.

Centralized Research Committee means a committee that includes representatives of all QEs in the SHIN-NY that is organized to review and approve Research proposals under which a researcher seeks information from more than one QE. The Centralized Research Committee shall meet the requirements set forth at 45 C.F.R. § 164.512(i)(1)(i)(B), meaning that the committee (1) has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the Research protocol on individuals' privacy rights and related interests; (2) includes at least one member who is not an employee, contractor, officer or director of a QE or any entity conducting or sponsoring the research, and is not related to any person who meets any of the foregoing criteria; and (3) does not have any member participating in a review of any project in which the member has a conflict of interest.

Certified Application means a computer application certified by a QE that is used by a Participant to Access Protected Health Information from the QE on an automated, system-to-system basis without direct Access to the QE's system by an Authorized User.

Community-Based Organization (CBO) means an organization, which may be a not-for-profit entity or government agency, which has the primary purpose of providing social services such as housing assistance, nutrition assistance, employment assistance, or benefits coordination. A Community-Based Organization may or may not be a Covered Entity.

Community Wide Deny* a form that is filled out by a patient to deny access to their health records to HealtheConnections Participants.

Consent Implementation Date means the date by which the NYS DOH requires QEs to begin to utilize an Approved Consent. In establishing such date, NYS DOH shall take into account the time that will be required for individual QEs to come into compliance with the Policies and Procedures regarding consent set forth herein.

Coroner means any individual elected to serve as a county's coroner in accordance with New York State County Law § 400.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

Covered Entity has the meaning ascribed to this term in 45 C.F.R. § 160.103 and is thereby bound to comply with the HIPAA Privacy Rule and HIPAA Security Rule.

Cybersecurity Policies and Procedures (CSPP) means the QE's and the State Designated Entities' set of policies and procedures that aim to protect the QE and SHIN-NY Enterprise's information systems and data.

Data Review Committee* consists of HealtheConnections employees that will review any research requests and either approve or deny them

Data Supplier means an individual or entity that supplies Protected Health Information to or through a QE. Data Suppliers include both Participants and entities that supply but do not Access Protected Health Information via the SHIN-NY (such as clinical laboratories and pharmacies). Government agencies, including Public Health Agencies, may be Data Suppliers.

Data Use Agreement* means an agreement that will establish who is permitted to use and receive data from HealtheConnections, along with allowable uses and disclosures of the data.

De-Identified Data means data that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Data may be considered de-identified only if it satisfies the requirements of 45 C.F.R. § 164.514(b).

Demographic Information means a patient's name, gender, address, date of birth, Social Security number, and other personally identifiable information, but shall not include any information regarding a patient's health or medical treatment or the names of any Data Suppliers that maintain medical records about such patient.

Disaster Relief Agency means (i) a government agency with authority under federal, state or local law to declare an Emergency Event or assist in locating individuals during an Emergency Event or (ii) a third-party contractor to which such a government agency delegates the task of assisting in the location of individuals in such circumstances.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. A QE engages in a Disclosure of information if the QE (i) provides a Participant with Access to such information and the Participant views such information as a result of such Access, or (ii) Transmits such information to a Participant or other third party.

Emancipated Minor means a minor who is emancipated on the basis of being married or in the armed services, or who is otherwise deemed emancipated under New York law or other applicable laws.

Emergency Event means a circumstance in which a government agency declares a state of emergency or activates a local government agency incident command system or similar crisis response system.

Emergency Medical Technician means a person certified pursuant to the New York State Emergency Services Code at 10 N.Y.C.R.R. §§ 800.3 and 800.6 as an emergency medical technician, an emergency medical technician-intermediate, an emergency medical technician-critical care, or an emergency medical technician-paramedic.

Failed Access Attempt means an instance in which an Authorized User or other individual attempting to Access a QE is denied Access due to use of an inaccurate log-in, password, or other security token.

Health Home means an entity that is enrolled in New York's Medicaid Health Home program and that receives Medicaid reimbursement for providing care management services to participating enrollees. **Health Home Member** means an entity that contracts with a Health Home to provide services covered by New York's Medicaid Health Home program.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

Health Information Exchange Organization means an entity that facilitates and oversees the exchange of Protected Health Information among Covered Entities, Business Associates, and other individuals and entities.

Health Oversight Agency has the meaning ascribed to thisterm in 45 C.F.R. § 164.501.

HIPAA means the Health Insurance Portability and Accountability Act of 1996.

HIPAA Privacy Rule means the federal regulations at 45 C.F.R. Part 160 and Subparts A and E of Part 164.

HIPAA Security Rule means the federal regulations at 45 C.F.R. Part 160 and Subpart C of Part 164.

HITECH means the Health Information Technology for Economic and Clinical Health Act. Independent Practice Association (IPA) means an entity that is certified as an independent practice association under 10 N.Y.C.R.R. § 98-1.5(b)(6)(vii).

Information Blocking Rules means the requirements and exceptions related to information blocking established by The Office of the National Coordinator for Health Information Technology set forth at 45 C.F.R. Part 171.

Insurance Coverage Review means the use of information by a Participant (other than a Payer Organization) to determine which health plan covers the patient or the scope of the patient's health insurance benefits.

ISC Sanctions Table* means a table that was developed by the (now defunct) SHIN-NY Policy Implementation Subcommittee to aggregate various non-compliance scenarios and provide examples of sanctions that may be appropriate, based on the various scenarios.

Level 1 Consent means a consent permitting Access to and receipt of Protected Health Information for Level 1 Uses in one of the forms attached hereto as Appendix A.

Level 2 Consent means a consent permitting Access to and receipt of Protected Health Information for a Level 2 Use in one of the forms attached hereto as Appendix B.

Level 1 Uses mean Treatment, Quality Improvement, Care Management, Utilization Review, and Insurance Coverage Reviews.

Level 2 Uses mean any uses of Protected Health Information other than Level 1 Uses, including but not limited to Payment, Research and Marketing.

Limited Data Set means Protected Health Information that excludes the 16 direct identifiers set forth at 45 C.F.R. § 164.514(e)(2) of an individual and the relatives, employers or household members of such individual.

Marketing has the meaning ascribed to this term under the HIPAA Privacy Rule as amended by Section 13406 of HITECH (42 USC § 17936).

Medical Examiner means a licensed physician who serves in a county medical examiner's office in accordance with New York State County Law § 400, and shall include physicians within the New York City Office of Chief Medical Examiner.

Minor Consent Services means those services for which a minor may provide their own consent without a parent's or guardian's permission, as permitted by New York State law, including but not limited to services provided pursuant to Public Health Law sections 2305 and 2504 and Mental Hygiene Law sections 22.11 and 33.21, or other applicable laws for certain types of health services (e.g., reproductive health, HIV testing, STD, mental health or substance use treatment) or services consented to by an Emancipated Minor.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

National Institute of Standards and Technology (NIST) Cybersecurity Framework means the set of industry standards and best practices to help organizations manage cybersecurity risks that has been developed by the National Institute of Standards and Technology. The NIST Cybersecurity Framework uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

NYS DOH means the New York State Department of Health.

One-to-One Exchange means a Transmittal of Protected Health Information originating from a Participant which has a relationship with a patient to one or more other Participants with the patient's knowledge and implicit or explicit consent where no records other than those of the Participants jointly providing health care or social services to the patient are Transmitted. Examples of a One-to-One Exchange include, but are not limited to, information provided by a primary care provider to a specialist when referring to such specialist, a discharge summary sent to where the patient is transferred, lab results sent to the Practitioner who ordered the laboratory test, or a claim sent from a Participant to the patient's health plan.

Organ Procurement Organization (OPO) means a regional, non-profit organization responsible for coordinating organ and tissue donations at a hospital that is designated by the Secretary of Health and Human Services under section 1138(b) of the Social Security Act (42 USC § 1320b-8[b]; see also 42 C.F.R. Part 121).

Participant means a Provider Organization, Payer Organization, Practitioner, Independent Practice Association, Accountable Care Organization, Public Health Agency, Organ Procurement Organization, Health Home, Health Home Member, Performing Provider System (PPS) Partner, PPS Lead Organization, PPS Centralized Entity, Social Services Program, Community-Based Organization, Social Care Network Lead Entity, or Disaster Relief Agency that has directly or indirectly entered into a Participation Agreement with a QE and Accesses Protected Health Information via the SHIN-NY.

Participation Agreement means the agreement made by and between a QE and each of its Participants, which sets forth the terms and conditions governing the operation of the QE and the rights and responsibilities of the Participants and the QE with respect to the QE.

Patient App means an application on a patient's smart phone, laptop, tablet, or other technology that collects Protected Health Information about the patient and makes such Protected Health Information accessible to the patient.

Patient Care Alert means an electronic message about a development in a patient's medical care, such as an emergency room or inpatient hospital admission or discharge, a scheduled outpatient surgery or other procedure, or similar event, which is derived from information maintained by a QE and is Transmitted by the QE to subscribing recipients but does not allow the recipient to Access any Protected Health Information through the QE other than the information contained in the message. Patient Care Alerts may contain demographic information such as patient name and date of birth, the name of the Participant from which the patient received treatment, and limited information related to the patient's complaint or diagnosis but shall not include the patient's full medical record relating to the event that is the subject of the electronic message.

Patient Consent Transition Rules means the rules set forth in Section 1.10.

Payment means the activities undertaken by (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or (ii) a health care provider or health plan to obtain or provide reimbursement for the provision of health care. Examples of payment are set forth in the HIPAA regulations at 45 C.F.R. § 164.501.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

Payer Addendum* is a document to be signed by Payer Organizations, which clarifies payer specific provisions governing access to patient data through HealtheConnections.

Payer Organization means an insurance company, health maintenance organization, employee health benefit plan established under the Employee Retirement Income Security Act of 1974 (ERISA) or any other entity that is legally authorized to provide health insurance coverage.

Practitioner means a health care professional licensed under Title 8 of the New York Education Law, or an equivalent health care professional licensed under the laws of the state in which the professional is practicing or a resident or student acting under the supervision of such a professional.

Personal Representative means a person who has the authority to consent to the Disclosure of a patient's Protected Health Information under Section 18 of the New York State Public Health Law and any other applicable state and federal laws and regulations.

Protected Health Information (PHI) means individually identifiable health information (e.g., any oral or recorded information relating to the past, present, or future physical or mental health of an individual; the provision of health care to the individual; or the payment for health care) of the type that is protected under the HIPAA Privacy Rule.

Provider Organization means an entity such as a hospital, nursing home, home health agency or professional corporation legally authorized to provide health care services.

Public Health Agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, the New York State Department of Health, a New York county health department or the New York City Department of Health and Mental Hygiene, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate and that has signed a Participation Agreement with a QE and Accesses Protected Health Information via the SHIN-NY.

QE Research Committee means a committee of a QE that is organized to review and approve Research proposals and which meets the requirements set forth at 45 C.F.R. § 164.512(i)(1)(i)(B), meaning that the committee (i.) has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the Research protocol on individuals' privacy rights and related interests; (ii.) includes at least one member who is not an employee, contractor, officer or director of the QE or any entity conducting or sponsoring the research, and is not related to any person who meets any of the foregoing criteria; and (iii.) does not have any member participating in a review of any project in which the member has a conflict of interest.

Qualified Entity Participation Agreement (QEPA) means the agreement between each of the QEs and the State Designated Entity that sets forth the terms and conditions for the QE participation in the SHIN-NY including providing QE Participants Access to and use of the SHIN-NY.

Qualified Entity (QE) means a not-for-profit entity that has been certified as a QE under 10 N.Y.C.R.R. Section 300.4 and has executed a contract to which it has agreed to be bound by SHIN-NY Policy Standards.

Quality Improvement means activities designed to improve processes and outcomes related to the provision of health care services. Quality Improvement activities include but are not limited to outcome evaluations; development of clinical guidelines; population-based activities relating to improving health or reducing health care costs; clinical protocol development and decision support tools; case management and care coordination; reviewing the competence or qualifications of health care

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

providers, but shall not include Research. The use or Disclosure of Protected Health Information for quality improvement activities may be permitted provided the Accessing and Disclosing entities have or had a relationship with the individual who is the subject of the Protected Health Information.

Record Locator Service or Other Comparable Directory means a system, that can be queried only by Authorized Users, that provides an electronic means for identifying and locating a patient's medical records across Data Suppliers.

Research means a systematic investigation, including research development, testing and evaluation designated to develop or contribute to generalizable knowledge, including clinical trials.

Retrospective Research means Research that is not conducted in connection with Treatment and involves the use of Protected Health Information that relates to Treatment provided prior to the date on which the Research proposal is submitted to an Institutional Review Board.

RHIO Administrator is the main point of contact for any communication with HealtheConnections. Refer to RHIO Administrator Roles and Responsibilities Sheet.

Sensitive Health Information means any information subject to special privacy protection under state or federal law, including but not limited to, HIV/AIDS, mental health, alcohol and substance use, reproductive health, sexually transmitted disease, and genetic testing information.

SHIN-NY means the technical infrastructure (SHIN-NY Enterprise) and the supportive policies and agreements that make possible the electronic exchange of clinical information among QEs, Participants, and other individuals and entities for authorized purposes, including both the infrastructure that allows for exchange among Participants participating in the same QE and the infrastructure operated by the State Designated Entity that allows for exchange between different QEs. The goals of the SHIN-NY are to improve the quality, coordination, and efficiency of patient care, reduce medical errors and carry out public health and health oversight activities, while protecting patient privacy and ensuring data security.

SHIN-NY Enterprise means the information technology (IT) infrastructure inclusive of the Qualified Entities (QEs) and the Statewide Data Infrastructure that supports the electronic exchange of patient health information across New York State.

SHIN-NY SOPs is the Standard Operating Procedures under the new Statewide Collaboration Process.

Social Care Network Lead Entity means an entity that is responsible under a contract with NYS DOH for establishing a network inclusive of Community-Based Organizations providing health-related social needs services to Medicaid enrollees as originally established as part of the New York Health Equity Reform (NYHER) program.

Social Services Program means a program within a social services district (as defined by New York Social Services Law, § 2) which has authority under applicable law to provide "public assistance and care" (as defined by New York Social Services Law § 2), Care Management, or coordination of care and related services.

sPRL means Statewide Patient Record Lookup, a system under which Protected Health Information or other information may be accessed across QE systems for disclosure to a Participant or other person who is permitted to receive such information under the terms of these Policies and Procedures.

State Designated Entity (SDE) means the public/private partnership in New York State that has been designated by the New York State Commissioner of Health as eligible to receive federal and state grants to promote health information technology.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

Statewide Chief Information Security Officer (CISO) means the senior-level executive employed by the State Designated Entity who has authority over the SHIN-NY Enterprise in order to establish and maintain the vision, strategy, and security program to ensure the SHIN-NY Enterprise's information assets and technologies are adequately protected.

Statewide Consent Registry (SCR)means the technical architecture to store patient consents collected by QEs and Participants.

Statewide Consent Management System means a system designed to track patient responses for Consent, including modifications to prior consent choices, and share those responses with QEs and Participants.

Statewide Data Infrastructure means the information technology infrastructure operated by or for the State Designated Entity that supports the aggregation of data provided by QEs and Participants, statewide reporting and analytics for public health activities and Medicaid purposes, and the exchange of information between QEs.

Telehealth means the use of electronic information and two-way, real-time communication technologies to deliver health care to patients at a distance. Such communication technologies include both audio-video and audio-only (e.g., telephonic) connections.

Transmittal means the sharing of Protected Health Information, a Limited Data Set, or De-identified Data to a recipient in either paper or electronic form, other than via the display of such information through the QE's electronic health information system or through a Certified Application.

Treatment means the provision, coordination, or management of health care and related services among health care providers or by a single health care provider, and may include providers sharing information with a third party. Consultation between health care providers regarding a patient and the referral of a patient from one health care provider to another also are included within the definition of Treatment.

Unsecured Protected Health Information means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services in guidance issued under section 13402(h)(2) of HITECH (42 USC 17932[h][2]).

Utilization Review means an activity carried out by a Payer Organization to determine whether a health care item or service that has been provided to an enrollee of such Payer Organization, or which has been proposed to be provided to such an enrollee, is medically necessary. *This policy is not intended to supersede or affect any state or federal laws related to Utilization Review. (See NY Insurance Law §4900(h) and Public Health Law §4900(8)).*

***** An asterisk denotes a term specific to HealtheConnections.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org