HealtheConnections Privacy and Security Policy and Procedures Handbook

May 2023

Introduction

The HEALTH ADVANCEMENT COLLABORATIVE OF CENTRAL NEW YORK, INC.("HAC-CNY"), a New York Not-for-Profit corporation d/b/a HealtheConnections ("HealtheConnections") 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. The scope of the Policies and Procedures includes 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"), along with other key stakeholders, through the Statewide Collaboration Process ("SCP"). It is the opinion of NYS DOH that the policies and procedures set forth are in compliance with state and federal laws.

It is the policy of HealtheConnections that each Authorized User be trained 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, 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 2 of the Terms & Conditions and will be distributed to the RHIO Administrator.

Table of Contents

Policy # P01: Compliance with Laws and Policies

I. Statement of Policy

HealtheConnections Participants must comply with all applicable federal, state, and local laws, rules and regulations and Policies and Procedures to provide essential privacy protections for patients and must implement appropriate internal policies and procedures for compliance therewith. HealtheConnections will monitor and enforce participant adherence to these policies. Any changes to the monitoring and enforcement of these policies will be reported to the NYS DOH and NYeC within 30 days.

II. Who Should Know This Policy

Each of the policies contained in the handbook applies to all Participants and Authorized Users that have registered with, and are participating in the exchange that may provide, make available, or request health information through the health information exchange. This also includes those that maintain and support system hardware and software.

III. Definitions

For definitions see Appendix A: Privacy and Security Policy Glossary

IV. Procedures

A. Law

1. SHIN-NY regulation requires that certain types of facilities are required to become a participant of a QE. These organizations can be found here: https://health.data.ny.gov/Health/Health-Facility-General-Information/vn5v-hh5r/data These facilities shall also connect to and share data through the QE. If a facility is unable to do so, they may apply for a waiver from the NYS DOH, which includes a plan for connectivity that is approved by HealtheConnections. A waiver will be valid for 6-9 months and HealtheConnections will monitor for progress.

   Other types of facilities are also eligible to participate in the SHIN-NY and will be vetted by the HealtheConnections' Account Management team.

2. Each Participant will, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. If applicable law requires that certain documentation exist or that other conditions be met prior to accessing Protected Health Information ("PHI") for a particular purpose, Participants shall ensure that they have obtained the required documentation or met the requisite conditions and shall provide evidence of such as applicable. SHIN-NY Privacy and Security Policies and Procedures apply to all Participants and can be found here: https://www.health.ny.gov/technology/regulations/shin-ny/docs/privacy_and_security_policies.pdf. In cases where the most recent version of these Policies and Procedures is silent or conflicts with SHIN-NY Privacy and Security Policies and Procedures, SHIN-NY Privacy and Security Policies and Procedures shall govern.

3. Each Participant that is not a Covered Entity, other than a public health authority or a health oversight agency under HIPAA (45 C.F.R. Sections 164.501 and 164.512[b] and [d]), such as a Community-Based Organization, that receives Protected Health Information shall adopt the administrative, physical and technical safeguards that are required under the HIPAA Security Rule related to such Protected Health Information and shall assess whether addressable safeguards under the HIPAA Security Rule should be adopted. In determining which addressable safeguards to adopt, such participants shall take into account their size, complexity, capabilities, and other factors

set forth under 45 C.F.R. Section 164.306(b). Nothing herein shall be construed to require Participants to comply with the HIPAA Security Rule and the HIPAA Privacy Rule with respect to information that does not constitute Protected Health Information.

a. HealtheConnections may conduct due diligence in regard to a Community-Based Organization that is not a Covered Entity that is seeking to become the QE's Participant and may reject such organization's request to become a Participant on the basis that the organization does not have sufficient security protocols, or any other reason related to privacy or security, so long as such reason does not constitute illegal discrimination. If a QE recognizes a Community-Based Organization that is not a Covered Entity as a Participant, then the requirements set forth in SHIN-NY Privacy and Security Policies and Procedures § 8.3. shall apply.

4. Each Participant will use reasonable efforts to stay abreast of any changes or updates to, and interpretations of, such laws and regulations to ensure compliance. This may include temporary waivers for Public Health and other emergencies issued by the New York State Department of Health.

B. Policies

1. Each Participant will, at all times, comply with all applicable Policies and Procedures.

2. Policies and Procedures may be revised and updated from time to time upon reasonable written notice to Participant. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Policies and Procedures.

3. Each Participant must identify at least one point of contact for communication with HealtheConnections (the "RHIO Administrator").

4. HealtheConnections offers core services as required and defined by SHIN-NY Policy, as well as additional services that may be fee-based.

C. Participant Policies

1. Each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and the Policies and Procedures.

2. In the event of a conflict between the Policies and Procedures and an institution's own policies and procedures, the Participant will comply with the policy that is more protective of individual privacy and security.

Policy # P02: Patient Consent - Level 1

I. Statement of Policy

New York State law requires that a QE shall not Disclose a patient's Protected Health Information via the SHIN-NY to a Participant unless the patient (or their personal representative) has provided an Affirmative Consent authorizing the Participant to Access or receive such Protected Health Information, unless an exception applies. From this point forward any reference to the patient consent also includes consent signed by a patient's personal representative. HealtheConnections does not allow alternative forms to the state approved Level 1 consent form.

II. Procedure

A. General Considerations

1. Unless an exception applies (see Section II-D through P), a patient's protected health information (PHI) cannot be disclosed through the SHIN-NY unless the patient has signed an Affirmative Consent approved by HealtheConnections authorizing the disclosure.

2. Affirmative Consent may be obtained electronically provided that there is an electronic signature that meets the requirements of the federal ESIGN statute, 15 U.S.C. § 7001 et seq., or any other applicable state or federal laws or regulations. See Electronic Signatures and Records Act (State Technology Law Article III, 9 N.Y.C.R.R. Part 540, New York State Office of Information Technology Services ESRA Guidelines NYS-G04-001).

3. An Affirmative Consent form is not required to name HealtheConnections on the form, provided that HealtheConnections reviews and approves the use of the form to ensure:
   a) The form is a state approved form and meets the requirements set forth in SHIN-NY Privacy and Security Policies and Procedures § 1.3.1 or § 1.3.2.
   b) The requirements established in SHIN-NY Privacy and Security Policies and Procedures § 1.3.5.f. are met.

4. An Affirmative Consent that applies to a Participant shall apply to (a) Authorized Users of the Participant and (b) an Affiliated Practitioner of the Participant provided that (i) such Affiliated Practitioner is providing health care services to the patient at the Participant's facilities; (ii) such Affiliated Practitioner is providing health care services to the patient in such Affiliated Practitioner's capacity as an employee or contractor of the Participant or (iii) such Affiliated Practitioner is providing health care services to the patient in the course of a cross-coverage or on-call arrangement with the Participant or one of its Affiliated Practitioners.

5. At a Participant's option and with HealtheConnections approval, an Affirmative Consent may apply to more than one Participant (e.g., a medical system gains consent on behalf of their associated facilities) provided that the consent form (i) lists each Participant with sufficient specificity to provide reasonable notice to the patient as to which Participant may access the patient's information via the health information exchange pursuant to such consent form and (ii) provides the patient with the option to select which of the Participants listed on the consent form may access the patient's information through the health information exchange; this option may be communicated verbally. Any Participant accessing information based on a consent form covering multiple Participants must be identified on such consent form at the time the patient grants Affirmative Consent. It is the responsibility of the Participants named on the consent

form to determine who and how the consent is maintained, including filing and entry into the health information exchange and its availability for audits.

6. At the time of consent, the Participant must advise the patient of:
   a) The intended use of the patient's health information that is obtained through the exchange.
   b) The ability to access a list of data suppliers by either logging into HealtheConnections website or by contacting HealtheConnections Support.

7. Patients need to be aware that, once they give consent, all of their health information will be available through the exchange. No partial or filtered data will be available.

8. If a patient consents, the information accessible through the exchange will include the following sensitive information and any re-disclosure of this information must comply with state and federal law:
   a) HIV-related information.
   b) Mental health information.
   c) Reproductive health information.
   d) Genetic testing information.
   e) Sexually transmitted disease information.
   f) Alcohol and substance use information.

9. All patient consents must be obtained using a Patient Consent Form approved by HealtheConnections. In addition, participants may also note the consent in their EHR system. Each Participant will maintain copies of all patients' written consents. See Appendix C for ways to access these forms.

10. Patients may change their consent at any time by completing a new patient consent form.

11. Patients may select consent for emergency treatment only (known as "Deny Consent except in a Medical Emergency"). This limits authorized users to access the patient's records in the health information exchange through "break the glass".

12. Patients may refuse to allow a Participant to access their health information through HealtheConnections (known as "Deny Consent") by completing the appropriate selection on the patient consent form. Patients may also deny access to all HealtheConnections participants ("Community-wide deny consent") by completing the HIE-wide consent form at the HealtheConnections office or at their provider's office, along with proof of identity. HealtheConnections will set the HIE-wide deny consent.

13. All patients' consents to payers must be in writing on the HealtheConnections Patient Consent Payer Consent Form. Each payer will maintain electronic or hard copies of all patients' written consents. See Appendix C for ways to access these forms.

14. Providers/Payers must not condition treatment/coverage on the patient's willingness to consent to the access of their health information through HealtheConnections.

15. Consent may be obtained electronically provided there is an electronic signature that meets the requirements of the federal ESIGN statute, 15 U.S.C. § 7001 et seq., or any other applicable New York State or federal laws or regulations.

16. A patient's consent is not time limited.

17. If a patient withdraws his/her consent, data that has been accessed by the Participant up to the time of withdrawal will remain as part of the Participant's records.

18. Participants will make reasonable efforts to comply with the American Disability Act when gaining patient consent.

B. Consent by Minors

1. It is the policy of HealtheConnections that a parent/guardian may consent for an under 18-year-old. With a parent/guardian's affirmative consent, a provider can access the minor's health record. If a parent/guardian has selected "No", "No, except in an emergency", or has not yet consented, the minor may override the consent if receiving minor consented services. Examples of minor consented services are reproductive planning, HIV/AIDS, STD testing, etc. The minor's override will only be in effect for the duration of that encounter.

2. Parents that share joint custody of the minor have equal authority to provide written consent for the minor.

3. If a court order clearly permits one parent to make health care decisions for a minor, that parent has the authority to provide written consent for the minor. If the court order is not clear as to which parent has the authority to make health care decisions, either parent may provide written consent for the minor.

4. As these policies relate to foster parents or other individuals who have legal custody (but not guardianship), Participants should follow Social Services Law §422, 422-a, 372, and 18 NYCRR § 357,432,441.

C. Consent of Minor Expires Upon Turning Eighteen

1. When the patient reaches the age of majority (18th birthday), the consent of his/her parent or legal guardian no longer applies.

2. When the patient reaches the age of majority (18th birthday), the consent of the patient as a minor no longer applies.

3. When the patient reaches the age of majority (18th birthday), the Participant must obtain the written consent of the (adult) patient in order to continue to access his/her health information through the exchange.

4. Access to any data after the 18th birthday will not be allowed until an Affirmative Consent has been obtained.

D. Exception to Affirmative Consent Requirement: Up-Loading Data

1. HealtheConnections holds patient data solely as a custodian of the Participants. HealtheConnections, as a business associate of the Participants, does not make patient information accessible to other Participants until patient consent is obtained.

2. Since the storage of data is not treated as a "disclosure" to a third-party requiring consent under New York law, Participants may upload patient information to HealtheConnections without patient consent.

E. Exception to Affirmative Consent Requirement: One-To-One Exchanges

1. One-to-One exchange is best described as a request by a Participant to receive specific information from or send specific information to an identified source with the patient's knowledge and implicit or explicit consent. Common examples include physician referrals, a discharge summary being sent by a treating hospital to the referring physician, or the delivery of lab results to the ordering practitioner.

2. Participants may receive One-to-One information via HealtheConnections services (e.g., Results Delivery, Alerts).

3. Each One-to-One exchange is understood and predictable to the patient, and information is limited in scope to records of Participants jointly providing health care or social services to the patient. Therefore, affirmative patient consent is not needed for a One-to-One exchange. However, if a patient requests limitation on the disclosure of his/her PHI to a Payer Organization, the practitioner must comply with this request.

4. NYS laws requiring written consent for release of sensitive information as identified in Section II-A-8 above still apply to the one-on-one exchange of health information. Providers should utilize their own consent forms for this purpose as applicable.

NOTE: The one-to-one exchange can only be done without Affirmative Consent, if the HIE technology has the capability to detect such exchange and only provide the PHI related to that exchange. Currently, the HIE technology that HealtheConnections uses can detect this exchange and only provide the information related to the exchange.

F. Exception to Affirmative Consent Requirement: Patient Care Alerts and Death Notifications

1. Patient Care Alerts:
   a) A Patient Care Alert may be Transmitted to a Participant without Affirmative Consent provided that the recipient of such Patient Care Alert is a Participant that provides, or is responsible for providing, Treatment or Care Management to the patient. Such categories of Participants may include, but are not limited to, Practitioners, Accountable Care Organizations, Health Homes, Payer Organizations, and home health agencies who meet the requirements of the preceding sentence. If a patient or a patient's Personal Representative affirmatively denies consent to a Participant to Access the patient's information, then Patient Care Alerts shall not be Transmitted to such Participant.
   b) Patient Care Alerts may be Transmitted from facilities subject to the New York Mental Hygiene Law without Affirmative Consent only if such alerts are sent to Payer Organizations, Health Homes, or other entities authorized by the New York State Office of Mental Health and the sending of such alerts otherwise complies with Mental Hygiene Law § 33.13(d).
   c) Patient Care Alerts shall be Transmitted in an encrypted form that complies with U.S. Health and Human Services Department Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

2. Death Notifications:
   a) Affirmative Consent shall not be required for HealtheConnections to Disclose the death of a patient to a Participant that (a) was responsible for providing Treatment or Care Management to such patient prior to the patient's death; or (b) is a Payer Organization that provided health coverage to the patient immediately prior to the patient's death. A death notification may only include Demographic Information and the date and time of death. Cause of death and information on the patient's diagnoses, health conditions, and treatments, as well as location of death, shall not be included in the death notification absent Affirmative Consent.

G. Exception to Affirmative Consent Requirement: Access to Patient Health Information in an Emergency Situation.

1. Affirmative Consent shall not be required for a Practitioner (or an HIE authorized user acting at the direction of the Practitioner) or Emergency Medical Technician (EMT) to access a patient's Protected Health Information through the health information exchange and these individuals may 'Break the Glass' if the following conditions are met:
   a) Treatment may be provided to the patient without informed consent because, in the Practitioner's or EMT's judgment, an emergency condition exists, the patient is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the patient's life or health.

b) The Practitioner or EMT determines, in his or her reasonable judgment, that information that may be held by or accessible through HealtheConnections may be material to emergency treatment.
c) No denial of consent to access the patient's information is currently in effect with respect to the Participant with which the Practitioner or EMT is affiliated.
d) Any non-Practitioner/non-EMT authorized user that accesses a patient's records using 'Break the Glass' under direction of a Practitioner must keep a record of the Practitioner under whose direction s/he acted.
e) The Practitioner, HIE authorized user acting at the direction of the Practitioner, or EMT, attests that all of the foregoing conditions have been satisfied.
f) The right to 'Break the Glass' terminates with the completion of an emergency treatment. If the user seeks to access the patient's health information after the emergency has ended, s/he must comply with patient consent requirements. If a patient's record contains Part 2 data, HeC will notify the Part 2 data supplier that their data may have been accessed.

2. Notwithstanding anything to the contrary set forth in these policies, HealtheConnections and its Participants shall not be required to exclude any Sensitive Health Information from access where the circumstances set forth in this Section G are met.

3. HealtheConnections will maintain a record of any 'Break the Glass' access.

H. Exception to Affirmative Consent Requirement: De-Identified Data

1. A QE may Disclose De-Identified Data without Affirmative Consent if the QE enters into a data use agreement with the recipient in accordance with section H.3, below, unless the QE determines that (a) such De-Identified Data is to be used to assist in Marketing activities that would not comply with the HIPAA Privacy Rule, or (b) the proposed use of the De-Identified Data is not in keeping with the mission of the SHIN-NY as described in 10 N.Y.C.R.R. § 300.1. Notwithstanding the foregoing, a data use agreement shall not be required if HealtheConnections is solely Transmitting to a third party that is designing a clinical trial or other clinical research study a count of the number of patients who appear to meet the inclusion and/or exclusion criteria being considered for such clinical trial or study, so long as there is no reasonable basis to believe that the count, when combined with the qualifying criteria, can be used to identify an individual.

2. Participants and business associates must comply with standards for the de-identification of data set forth in 45 C.F.R. § 164.514.

3. HealtheConnections shall ensure that a data use agreement required under this section:

a) Establishes the permitted uses of the De-Identified Data by the recipient and prohibits the recipient or any third parties from using the De-Identified Data for any purposes other than the permitted uses, unless otherwise required by law.
b) Prohibits the recipient from re-identifying or attempting to re-identify the De-Identified Data.
c) Provides the QE, or a Participant who holds Protected Health Information that was used in whole or in part to create the De-Identified Data set, with a right to audit the practices of the recipient regarding ensuring the data is not re-identified.
d) Requires the recipient to report to the QE if the recipient has knowledge that the De-Identified Data has been re-identified or if there have been any other violations of the data use agreement.
e) Mandates that the recipient may not disclose the De-Identified data to any third party unless the agreement explicitly permits such a Disclosure, and the third party also agrees in writing to follow the restrictions set forth in this Section H.3.

4. Any Disclosures of De-Identified Data shall comply with any applicable terms in the Business Associate Agreement between the QE and the Data Suppliers that are the source of the De-Identified Data.

5. Participants should have and follow their own internal policies when determining access to de-identified information and for what purpose.

I. Exception to Affirmative Consent Requirement: Public Health Reporting

1. A Public Health Agency may access PHI through HealtheConnections' clinical viewer or portal for the following public health purposes without affirmative consent:

    a) To investigate suspected or confirmed cases of communicable disease.
    b) To ascertain source of infection.
    c) To seek out contacts or take steps to reduce morbidity and mortality.
    d) To investigate suspected or confirmed cases of lead poisoning.
    e) For other public health purposes authorized by law and approved through the Statewide Collaboration Process.
    f) Additional purposes and details are listed in SHIN-NY Privacy and Security Policies and Procedures § 1.2.2.

2. If a Data Supplier or Participant is permitted to Disclose Protected Health Information to a government agency for purposes of public health reporting without patient consent under applicable state and federal laws and regulations, HealtheConnections may make that Disclosure on behalf of the Data Supplier or Participant without Affirmative Consent.

3. HealtheConnections may Disclose Protected Health Information without Affirmative Consent to the New York State Office of Mental Health ("OMH") for the following public health purposes if HealtheConnections Discloses Protected Health Information to NYS DOH in its role as a Public Health Agency and OMH is authorized to obtain such information under applicable state and federal law. Such public health purposes shall consist of investigations aimed at reducing morbidity and mortality, monitoring of disease trends, and responding to public health emergencies.

4. A patient's denial of consent for all Participants in HealtheConnections to access the patient's PHI shall not prevent or otherwise restrict a Public Health Agency from accessing the patient's PHI through HealtheConnections.

5. Public Health users will not have access to 42 CFR Part 2 (Substance Use Disorder) patient data per SAMHSA Rule.

J. Exception to Affirmative Consent Requirement: Improvement and Evaluation of HealtheConnections Operations

1. An Affirmative Consent is not required for HealtheConnections, government agencies or their contractors to access PHI through the exchange for the purpose of evaluation and improvement of the HealtheConnections QE operations.

2. This is limited to the minimum necessary information required to accomplish the intended purpose of the use or disclosure.

K. Exception to Affirmative Consent Requirement: Indication of Medical Orders of Life Sustaining Treatment ('MOLST')

1. HealtheConnections may note whether a patient has signed a MOLST without Affirmative Consent through its Record Locator Service or other Comparable Directory.

L. Exception to Affirmative Consent Requirement: Organ Procurement Organization Access

1. A QE may provide an Organ Procurement Organization with access to PHI without affirmative consent solely for the purposes of facilitating organ, eye, or tissue donation and transplantation.
2. A patient's denial of consent for all Participants in a QE to access the patient's PHI shall not prevent or otherwise restrict an Organ Procurement Organization from accessing the patient's PHI through a QE.

M. Exception to Affirmative Consent Requirement: Disclosures to NYS DOH Regarding Medicaid beneficiaries.

1. Affirmative Consent shall not be required for a QE to Disclose Protected Health Information of Medicaid beneficiaries to NYS DOH or a Business Associate of NYS DOH to the extent such Disclosure is necessary to
   a) calculate performance under quality measures adopted by the New York State Medicaid program; or
   b) determine payments to be made under the New York State Medicaid program.

N. Exception to Affirmative Consent Requirement: Disclosures to Health Plans/Payers for Quality Measures.

1. Affirmative Consent shall not be required for QE to disclose PHI to a Payer Organization (including NYS DOH in regard to its operation of the New York State Medicaid program) or a Business Associate of a Payer Organization to the extent such disclosure is necessary to (i) calculate performance of HEDIS or QARR measures; or (ii) in the case of disclosures to NYS DOH, determine payments to be made under the New York State Medicaid program.

O. Exception to Affirmative Consent Requirement: Telehealth

1. Generally. Affirmative Consent shall not be required for a QE to disclose a patient's Protected Health Information to a Participant that provides telehealth services to such patient if:
   a) The Participant has asked the patient if the Participant may Access or receive the patient's Protected Health Information, and the patient has verbally consented to such request.
   b) The Participant uses the Protected Health Information only for Level 1 purposes.
   c) The Participant keeps a record of the patient having provided verbal consent, which may take the form of a notation in the electronic record of such consent, an audio recording of the consent, or another appropriate means of recording consent.
      i. The Participant does not Access or receive any Protected Health Information subject to 42 C.F.R. Part 2 or Mental Hygiene Law §33.13 unless the patient has provided consent in written or electronic form and a signature that is recognized by the Electronic Signatures and Records Act, including an audio signature recording to the extent under the act.
      ii. The Participant Accesses or receives the patient's Protected Health Information only during the time period specified in subsection 2.

1. Duration of telehealth verbal consent. The patient's verbal consent shall remain valid until the patient has an in-person encounter with the Participant or revokes

consent, provided that the Participant:

i. Informs the patient that the consent will persist until the patient has an in-person encounter with the Participant or revokes consent.
ii. Informs the patient of the patient's right to revoke consent by notifying the Participant of such revocation either verbally or in writing; and
iii. Provides the patient with access to a written consent form that documents the terms of the verbal consent by either providing the patient with a copy of the form (via email, text, mail or otherwise) or an electronic link to such form.

The Participant shall keep a record of having provided such information to the patient. If the Participant fails to comply with requirements (a) through(c) above, the Participant shall expire the verbal consent after 72 hours. Otherwise, the Participant shall expire the consent upon the patient's next in-person encounter.

P. Exception to Affirmative Consent Requirement: Disclosures for Disaster Tracking.

1. For the purpose of locating patients during an Emergency Event, HealtheConnections may Disclose to a Disaster Relief Agency limited patient information without Affirmative Consent in accordance with SHIN-NY Privacy and Security Policies and Procedures § 1.2.3.
   a) The information disclosed pursuant to this exception shall be limited to the Minimum Necessary.

2. A patient's denial of consent for all Participants in a QE to Access or receive the patient's Protected Health information by signing a Community-wide-deny (a HealtheConnections form that allows a patient to deny access to all HealtheConnections participants) shall not restrict a QE from disclosing information to a Disaster Relief Agency as permitted by this section.

Policy # P03: Patient Consent - Level 2

I. Statement of Policy

A separate and distinct Level 2 Consent Form must be used by Participants which includes provider organizations, payer organizations, and practitioners for any other use of data outside of Treatment, Quality Improvement, Care Management, and Insurance Coverage Reviews. HealtheConnections does not allow alternative forms to the state approved Level 2 consent form.

II. Procedure

A. Patients must sign a Level 2 Consent Form in order for the Participant to use data for purposes other than treatment, quality improvement, care management, and insurance coverage reviews.

B. This form is time limited and must expire within 2 years of signing.

C. A patient can revoke this consent at any time.

Policy # P04: Authorized User Roles and Management

I. Statement of Policy

A. Authorized Users of the health information exchange. HealtheConnections' Participants who may access the health information exchange* shall confirm the identity of and assign the appropriate role to each of their Authorized Users before access can be granted. Users shall be permitted access to the health information exchange only where such access is consistent with the user's role within the organization. The following are the Authorized User roles associated with the health information exchange:

   a. Break the Glass Practitioner or Authorized User acting under the direction of a Practitioner; or Emergency Medical Technician who has temporary rights to access PHI for that patient.
   b. Practitioner with access to clinical and non-clinical information
   c. Non-practitioner with access to clinical and non-clinical information
   d. Non-practitioner with access to non-clinical information
   e. QE administrator with access to non-clinical information
   f. QE administrator with Public Health access
   g. QE Administrator with bypass consent access for operational purposes
   h. Public Health

*A Participant that is a Community-Based Organization and not a Covered Entity may not Access Protected Health Information via the health information exchange and instead may only receive Transmittals of Protected Health Information via direct or another encrypted means of communication.

B. Users of Direct Mail and Patient Care Alerts. HealtheConnections' Participants who (i) access Direct Mail and/or (ii) receive Patient Care Alerts shall confirm the identity of each user. Users shall be permitted to access Direct Mail and/or Patient Care Alerts only where such access is consistent with the user's role within the organization.

C. Provisioning of authorized users consistent with this policy is managed by HealtheConnections support.

II. Procedures

A. The Participant's RHIO Administrator(s) will identify and manage their authorized users' roles and communicate the same to HealtheConnections by completing the applicable form(s): (i) Authorized User Certification and Application form, (ii) Direct Mail User form, (iii) myAlerts User form.

B. HealtheConnections will set up the user accounts per the approved form received from the Participant's RHIO Administrator.

C. The RHIO Administrator will manage the administration of all HIE authorization for their authorized users.

Policy # P05: Certification of Authorized Users

I. Statement of Policy

It is required that HealtheConnections Participant's designated Authorized Users, prior to becoming an Authorized User and annually thereafter, be trained regarding the HealtheConnections privacy and security policies. Once trained, each Authorized User of the exchange must sign an Authorized User Certification and Application form acknowledging that they have been trained on HealtheConnections' policies. These forms must remain on file at the Participant's organization for at least 6 years.

II. Procedures

A. Participants will ensure that each of their proposed authorized users complete HealtheConnections-sponsored or approved training.

B. Participants will manage the signing and maintenance of the user forms.

C. All forms will remain on file with the Participant for at least 6 years.

Policy # P06: Authentication Level and Management

I. Statement of Policy

It is required that the exchange meet, at minimum, an Authenticator Assurance Level 2 (AAL2) set forth in National Institute of Standards and Technology Special Publication 800-63 (hereinafter, "NIST SP 800-63"). standard for authentication of each Authorized User. This requires proper identification prior to assignment of a unique username and password to enter the system. Passwords shall meet the requirements stipulated in SHIN- NY Privacy and Security Policies and Procedures.

II. Procedures

A. HealtheConnections representative will meet with the Participant's designated RHIO Administrator prior to implementing QE processes at the participating organization.

B. HealtheConnections shall authenticate, or shall require its Participants to authenticate, each Authorized User's identity prior to providing such Authorized User with Access to Protected Health Information via the SHIN-NY

C. Upon proper identification of the Authorized User, the Participant's RHIO Administrators can request access to the HIE for the Authorized User.

1. Group or temporary usernames shall be prohibited.

2. 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.

D. Password policy will be enforced through configuration settings in the HIE software.

1. Passwords shall meet the password strength requirements set forth in the NIST SP 800-63 guidelines, as may be revised periodically.

2. Authorized Users shall be required to change their passwords in accordance with the NIST SP 800-63 guidelines, as may be revised periodically.

Policy # P07: Business Associate Agreements

I. Statement of Policy

A Business Associate Agreement will be executed between HealtheConnections and the Participant which will set forth the terms and conditions governing the use and disclosure of PHI as specified in standards for privacy of individually identifiable health information in 45 CFR 164.501(e)(1).

II. Procedures

A. Each Participant will sign a Business Associate Agreement with HealtheConnections.

B. It will be HealtheConnections' discretion as to whether the Business Associate Agreement is that provided by HealtheConnections or the Participant.

Policy # P08: Minimum Necessary Access – Other Than Use for Treatment

I. Statement of Policy

HealtheConnections' Participants must comply with applicable law and the Policies and Procedures and promulgate the internal policies required for such compliance in order to provide essential privacy protections for patients.

II. Procedure

A. Uses

1. All Participants must ensure that reasonable efforts are made, except in cases of Treatment, to limit the information accessed through the exchange to the minimum amount necessary to accomplish the intended purpose for which the information is accessed.

2. Each Participant must identify that person or class of persons as appropriate, in its workforce, including physicians and their staff, who need access to protected health information to carry out their duties.

B. Disclosures

1. Each Participant will disclose through the exchange only the minimum amount of health information necessary for the purpose of disclosure.

2. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

3. Disclosures to Death Investigators shall not require Affirmative Consent for the purpose of determining the cause of a patient's death provided that all of the following are met:
   a. The receiving Participant is a licensed physician or nurse practitioner whose professional responsibilities include determining the cause of death of a patient. Such Practitioners may include Medical Examiners and Coroners who are licensed as physicians or nurse practitioners.
   b. Death Investigators shall access the Minimum Necessary PHI to accomplish their purpose.
   c. Protected Health Information originating from a facility subject to the New York Mental Hygiene Law is disclosed only if the facility has requested that an investigation be conducted into the death of a patient and the recipient is a Medical Examiner or Coroner that is licensed as physician or nurse practitioner.

C. Requests

1. Each Participant will request only the minimum amount of health information through the exchange as is necessary for the intended purpose of the request.

2. This Minimum Necessary Policy does not apply to requests by health care providers for treatment purposes.

D. Entire Medical Record

1. A Participant will not use, disclose, or request an individual's entire medical record except where specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

2. This limit does not apply to disclosures to or request by a health care provider for treatment purposes or disclosures required by law.

3. Each Participant should follow its own internal policies to determine what PHI is reasonably necessary.

Policy # P09: Access Policies to HIE

I. Statement of Policy

HealtheConnections Support manages access to the HIE. A Participants' RHIO Administrator will submit a request for an account for an approved authorized user for that participant's organization.

II. Procedures

A. HealtheConnections Support will create a Username and Password upon receipt of an approved Authorized User Certification and Application form. The Authorized User will be prompted to set security questions and to change their password upon initial entry.

B. A user will be allowed three (3) attempts. If the user fails to access the system after three attempts, the user will be locked out of the system. The user can then use the "Forgot Password" button, which will send an email with a link to answer security questions. The user may also contact HealtheConnections Support to re-set their password. HeC Support will request identifying information and then send a link to the user's email to reset their password.

C. Passwords are expired every 90 days and the Authorized User will be prompted to re-set their password.

Policy # P10: Termination of Access

I. Statement of Policy

It is required that access is terminated within one business day of the following:

a. Termination of a Participation Agreement
b. Termination of an Authorized User's employment or affiliation with a Participant
c. As an outcome of a Breach Sanction per P19: Sanctions for Breach

II. Procedures

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 Operations Support, **in writing**, as promptly as reasonably practicable. HealtheConnections Operations Support will terminate access for the named Authorized User within one business day of notification.

Policy # P11: Amendment of Data

I. Statement of Policy

HealtheConnections Participants shall comply with applicable federal, state, and local laws as well as HIPAA regulations regarding an individual's right to request amendment and/or correction of protected health information.

II. Procedure

A. If erroneous patient PHI was due in part to data aggregation and exchange activities done by HealtheConnections, HealtheConnections shall identify the root cause of the error and ensure its correction. HealtheConnections shall log all such errors, the actions taken to address them, and the final resolution of the error. HealtheConnections shall make reasonable efforts to identify Participants that accessed or received such erroneous information and to notify them of corrections.

B. All other requests for amendments and/or corrections must go through the data source Participant.

1. If an individual requests, and the Participant accepts, an amendment to the health information about the individual, the Participant shall make reasonable attempts to inform other primary care Participants that accessed or received such information through the health information exchange.

C. These provisions do not apply to updates to data that are made by Data Suppliers in the ordinary course of their clinical activities, nor do they apply to updates to Demographic information.

Policy # P12: Audit Logs

I. Statement of Policy

It is required that HealtheConnections maintain audit logs of the HIE that contain, at minimum, the following information:

a. The identity of the patient whose Protected Health Information was accessed or transmitted.
b. The identity of the Authorized User accessing Protected Health Information or recipient of a transmittal of Protected Health Information.
c. The identity of the Participant with which such Authorized User is affiliated.
d. The type of Protected Health Information or record accessed (e.g., pharmacy data, laboratory data, etc.) or transmitted.
e. Date and time of access or transmittal.
f. The source of the Protected Health Information (i.e., the identity of the Participant from whose records the accessed or transmitted Protected Health Information was derived).
g. Unsuccessful access (log-in) attempts.
h. Whether access occurred through a Break the Glass incident.

These logs are required to be immutable and kept for at least 6 years from the date of access.

II. Procedures

A. Audit logs will be produced and maintained through the health information exchange software.

III. Exceptions

A. There is no audit log requirement if the QE transmits PHI based on written instructions without modifying it (e.g., data forwarding).

B. There is no audit log requirement if the QE performs analytics on behalf of a participant and a patient's name is returned in response to a query and such result is never supplied to a participant.

Policy # P13: Request for Audit Logs by a Participant

I. Statement of Policy

It is required that HealtheConnections fulfill any request for audit logs within 10 calendar days to any Participant. The audit log will contain the following information regarding the patient that was accessed:

a. The name of each Authorized User who accessed such patient's Protected Health Information in the prior 6year period.
b. The time and date of such access.
c. The type of Protected Health Information or record that was accessed (i.e., clinical data, lab data, etc.).

II. Procedures

A. Audit logs will be produced and maintained in the health information exchange software.

B. Participants will only be entitled to such an audit log for patients who have provided affirmative consent for that Participant to access his/her Protected Health Information.

C. Participants will contact HealtheConnections Operations Support for such a request.

Policy # P14: Request for Audit of Accesses or Records by a Patient

I. Statement of Policy

It is required that HealtheConnections fulfill any request for audit of accesses or records within 10 business days.

Patient Records Accessed Report contains:

a. The Participant through which an Authorized User accessed Protected Health Information in the prior 6-year period.
b. Patient Name
c. Patient Date of Birth
d. The date and time of each access.
e. The type of Protected Health Information or record that was accessed (e.g., clinical data, lab data, etc.).

Consent Report contains:

a. Participant Name
b. Patient Name
c. Patient Date of Birth
d. History of consent options for that Participant
e. Effective date of the consent option
f. Date and time the consent was created.
g. Method by which the consent was created in HealtheConnections.

Patient Records Report contains:

a. A complete listing of the patient's clinical records, imaging notes, and transcriptions maintained by HealtheConnections.

II. Request Procedures

Audit Report Request Procedures:

A. Patients will contact HealtheConnections for such a request. The request form and policy for making such requests are available on our website under Resources / For Patients, or by contacting HealtheConnections Support at 315-671-2241 x5.

B. Patients may request one free paper, PDF or XLS audit report every 12 months. For other/additional requests, a fee may be assessed to cover the HealtheConnections' reasonable costs. Before imposing any such fee, HealtheConnections will first inform the patient of the fee and provide the patient an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

C. The following types of disclosures are exempt from the accounting requirements set forth in this policy:

1. Disclosures to the individual of their own PHI.
2. Disclosures made pursuant to an authorization from the individual.
3. Disclosures for HealtheConnections' operations, e.g., to conduct a Participant audit.
4. Disclosures that are incident to a permitted use and disclosure, e.g., to fulfill an individual's request(s).
5. Disclosures made prior to six years before the date of the request.

D. The Participant will be notified of a patient request if the Authorized User is named in the audit report.

Records Request Procedures:

A. Patients will contact HealtheConnections for such a request. The request form and policy for making such requests are available on our website under Resources/ For Patients, or by contacting HealtheConnections Support at 315-672-2241 x5.

B. Patients may request one free paper, PDF, or XML report of their records every 12 months. For other/additional requests, a fee may be assessed to cover HealtheConnections' reasonable costs. Before imposing any such fee, HealtheConnections will first inform the patient of the fee and provide the patient an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

C. A report of a patient's records will be produced via a query procedure in the health information exchange database. Information included will be everything per USCDI Data Classes and Elements that HeC has, except for:
    1. Psychotherapy notes, which are the personal note of a mental health care provider documenting or analyzing the contents of a counseling session, that are maintained separate from the rest of the patient's medical record.
    2. Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative action or proceeding.
    3. Minor consented services data for minors under the age of 18 – if this data cannot be excluded, then none of the minor data shall be provided.

Policy # P15: Periodic Audits

I. Statement of Policy

It is required that HealtheConnections or each Participant conducts audits. Each participant is required to complete the following audits, as applicable:

A. Public Health Participants that bypass consent will be audited weekly for the following:
   1. Patient Records Accessed by authorized users with the Public Health role.

B. Organ Procurement Participants that bypass consent will be audited weekly for the following:
   2. Patient Records Accessed by authorized users.

A. All other Participants will be audited annually for the following:
   1. A sample of Patient Affirmative Consents on file
   2. Patient Records Accessed by authorized users.

B. Break-the-Glass accesses are audited daily.

HealtheConnections has the authority to conduct random consent audits on its Participants.

II. Procedures

HealtheConnections generates audit reports and notifies participants of their obligation to review and attest to their audit.

A. Public Health participants shall attest that authorized users that bypass consent have appropriately accessed patient records for Public Health purposes.

B. Organ Procurement participants shall attest that authorized users that bypass consent have appropriately accessed patient records for Organ Procurement purposes.

C. All other participants will be required to:
   1. Maintain proof and attest to HealtheConnections that an Affirmative Consentform is on file for a list of patients on a statistically significant sample size that will be produced by HealtheConnections.
   2. Attest that all accesses by Authorized Users have been appropriate in the course of patient care.

D. Any participant that uses Break-the-Glass functionality will be required to attest daily that accesses were appropriately made in an emergency situation.

E. Failure to respond within the requested time period will result in follow-up to the Audit Contact. Continued lack of response will result in sanctions such as retraining, escalation within Participant leadership, and/or a request to remove and replace the AuditContact.

Policy # P16: Public Availability of Audits

I. Statement of Policy

It is required that HealtheConnections makes results of the audits available.

II. Procedures

A. HealtheConnections posts quarterly and annual audit results on the HealtheConnections website.

Policy # P17: Privacy Complaints and Concerns

I. Statement of Policy

Each HealtheConnections Participant shall have a mechanism for, and shall encourage all workforce members, agents, and contractors to report any non-compliance with these policies to the Participant. Each Participant also shall establish a process for individuals whose health information is included in the HealtheConnections HIE to report any non-compliance with these Policies or concerns about improper disclosures of information about them.

II. Procedures

A. Any complaints/concerns about confidentiality will be reported to the affected entity's HIPAA Privacy Officer for standard follow-up.

B. On completion of the investigation, the Participant will notify HealtheConnections Operations Support of such complaint/concern, to the extent allowable under the Participant's own policies.

C. Steps to mitigate could include, among other things, data source Participant notification to the individual of the disclosure of information about them, or Participant requests to the party who received such information to return and/or destroy the disclosed information. See Policy # P18: Breach Response.

D. HealtheConnections Support will archive the summaries of the complaints/reports for later reporting and discussion.

E. In the event that a Participant or HealtheConnections associate feels there is a complaint or concern that suggests HealtheConnections' investigation of the complaint/concern is a conflict of interest, it will be reported to the Chair of the HealtheConnections' Board.

Policy # P18: Breach Response

I. Statement of Policy

HealtheConnections and its Participants are responsible for immediately investigating and mitigating, to the extent possible, any breach of Unsecured PHI.

II. Procedures

A. Periodic Audits must be conducted by HealtheConnections.

1. HealtheConnections must conduct and publish audits at least annually and submit audit reports, including identification of Breaches, to the Board. See Policy # P15: Periodic Audits.

B. Upon discovery of a Breach of Unsecured PHI by a HealtheConnections Participant, the following process will be followed:

1. The Participant will:
   a) Investigate the scope and magnitude of the Breach.
   b) Identify the root cause of the Breach.
   c) Notify HealtheConnections Operations Support of the Breach and mitigation plan in the most expedient time possible and without unreasonable delay, to the extent that the Participant policies allow.
   d) Mitigate the Breach to the extent possible.
   e) If applicable, request the party who received such information to return and/or destroy the impermissibly disclosed information.
   f) Apply sanctions to Participant Authorized Users based on internal policies.
   g) Submit final report to HealtheConnections Policy and Compliance officer to the extent that the Participants policies allow.

2. Steps to mitigate must include, among other things, Participant notification to the individual of the disclosure of information about them and notification to regulatory agencies in compliance with the state and federal laws, rules, and regulations that govern their entity.

C. Upon discovery, by a HealtheConnections staff member or vendor, of a Breach of information systems, the following steps will be taken, unless otherwise stated in their Business Associate Agreements:

1. HealtheConnections will:
   a) Immediately notify the Participant of the Breach or potential Breach.
   b) Collaborate with the Participant in investigating the Breach, determine the causative factors, and establishing a mitigation plan.
   c) Request the Participant to perform a risk analysis to determine the financial, reputational, or other harm to the patient potentially caused by the Breach.
   d) Collaborate with the participant to send letters within 60 days that the Breach became known by HealtheConnections to affected patients of the Participant.
      i. If the Breach involves multiple Participants and it is unclear as to whom the Breached information relates, all potentially affected Participants will be notified.
      ii. Determine type of notifications to be made and responsibility for costs of notifications.
   e) Mitigate the Breach to the extent possible.
   f) If applicable, request the party who received such information to return and/or destroy the impermissibly disclosed information.
   g) Apply sanctions as appropriate (see Policy # P19: Sanctions for Breach).

h) Submit a final report.
i) Notify the HealtheConnections Board of Directors of the Breach.

2. Steps to mitigate must include, among other things, Participant notification to the individual of the disclosure of information about them and notification to regulatory agencies in compliance with the state and federal laws, rules, and regulations that govern their entity.

3. In the event that a Participant or HealtheConnections associate feels there is a breach that suggests the HealtheConnections' investigation of Breach is a conflict of interest, it should be reported to the Chair of the HealtheConnections' Board.

D. Breach Notification

1. Upon discovery of a Breach, the Participant or HealtheConnections must notify either through written notification by first class mail or by electronic mail, if specified to the individual, to each individual (or next of kin if individual is deceased) whose protected health information has been or is reasonably believed to have been accessed, acquired, or disclosed as a result of a Breach through the exchange. The notification should be sent to the last known address of the individual or next of kin.
   a) Substitute notice (e.g., posting on a website) may be provided if there is insufficient or out of date contact information that precludes direct written or electronic notification. In cases of 10 or more individuals for which there is insufficient or out of date contact information, a posting on any Covered Entity's website for at least 90 days or notice in major print or broadcast media is required. In either case, a toll-free number must be provided.

2. In cases that the entity deems urgent based on the possibility of imminent misuse of PHI, notice by telephone or other method is permitted in addition to the above methods.

3. The Participant (in some cases, HealtheConnections) must notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number or persons affected.

4. If the Breach is suspected to involve more than 500 residents of a particular state or jurisdiction, notice must also be made to media outlets and the Secretary of Health and Human Services. This will require that the SHIN-NY Communications Plan be invoked.

5. Notification of any Breach should be made in the most expedient time possible and without reasonable delay and in no case later than 60 calendar days after discovery and investigation of the Breach.

6. Notification should include, to the extent possible, the following:
   a) A brief description of what happened, including the date of the Breach and the date of the discovery, if known.
   b) A description of the types of unsecured protected health information that were involved in the Breach (e.g., name, SS#, address, etc.).
   c) The steps individuals should take to protect themselves from potential harm resulting from Breach.
   d) A brief description of what the Participant involved is doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches.
   e) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or portal address.

Policy # P19: Sanctions for Breach

I. Statement of Policy

Each HealtheConnections' Participant shall implement their system procedures to discipline and hold workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request protected health information except as permitted by these policies and procedures and that they comply with these policies and procedures.

II. Procedures

A. Sanctions for Breaches Reported to Participant

1. Sanctions for Breach should be handled according to the individual Participant's HIPAA Privacy & Security Policies.

2. Participants have a duty to report any violations of the Policies and Procedures to the privacy officer of the affected entity as well as to HealtheConnections, as permitted by Participants policies.

3. Such discipline measures should be based on the level of severity and intent of the Breach and include, but not be limited to, verbal and written warnings, re-training requirements, termination of participation in the exchange, and possible termination of employment as determined by the Participant.

B. Sanctions for Breaches Reported to HealtheConnections

1. HealtheConnections will report any violations reported to HealtheConnections to the affected Participant if the Participant was not the source of the report.

2. After investigation, discipline measures will be taken on a case-by-case basis based on the level of severity and intent of the Breach. These sanctions may include, but are not limited to:
   a) Re-training on the policy and procedures.
   b) Verbal or written warnings.
   c) Reduced access for an Authorized User.
   d) Suspension of access for an Authorized User.
   e) Termination of access for an Authorized User.
   f) Suspension of access for all Participants Authorized Users.
   g) Termination of Participation Agreement.

C. Other Sanctions

1. In the event that a Breach is reported to the Chair of the HealtheConnections' Board due to a conflict of interest in HealtheConnections' investigation of the Breach or a suspected Breach by a HealtheConnections associate, sanctions will be determined by the HealtheConnections' Board. These sanctions may include all of the above in addition to:
   a) Suspension of a HealtheConnections associate.
   b) Termination of a HealtheConnections associate.

Policy # P20: Patient Engagement and Access

I. Statement of Policy

It is required that HealtheConnections and its Participants educate patients on the consent process and the terms and conditions on which their Protected Health Information is shared. HealtheConnections is required to conform to any patient education standards that are developed through New York State.

HealtheConnections shall facilitate the access of patients and their Personal Representatives to patients' Protected Health Information maintained by the HealtheConnections through one of the following mechanisms:

A. HealtheConnections' own web-based portal or Participants' web-based portals.

B. A web-based portal established by or maintained by a third party on behalf of a patient, including a Patient App, provided the requirements related to disclosures to third parties are met.

C. A paper or electronic copy of information maintained about the patient by HealtheConnections.

D. Any other mechanism requested by the patient (provided that HealtheConnections need not provide the Protected Health Information via the requested mechanism if applicable law, including the Information Blocking Rules, permit HealtheConnections to use an alternative mechanism).

HealtheConnections shall have the means of receiving and responding to requests from patients and Personal Representatives to disclose such patients' Protected Health Information to third parties, including but not limited to Patient Apps, friends and family of patients, and legal representatives of patients pursuant to SHIN-NY Privacy and Security Policies and Procedures § 5.3.

II. Procedures

A. HealtheConnections will develop and distribute educational materials including consent forms and informational brochures to Participants.

B. Participants are required to support HealtheConnections' efforts in their office by providing these materials to their patients.

C. HealtheConnections will appoint at least one consumer representative to its Board of Directors.

Policy # P21: Request for Disclosure Restriction to Payer Organizations

I. Statement of Policy

In accordance with HIPAA and HITECH, HealtheConnections will allow for patients to restrict the disclosure of certain PHI, even when an Affirmative Consent has been executed, to Payer organizations.

II. Procedures

A. Upon the Participant's receipt of a patient's request that PHI created by that Participant not be disclosed to a Payer Organization, any Affirmative Consent previously granted to such Payer Organization is revoked and such revocation remains in effect permanently unless and until the patient's request is withdrawn.

B. Upon receipt of an Affirmative Consent covering a Payer Organization, the Payer Organization or QE must notify the patient in writing that his/her provision of the Affirmative Consent will revoke any prior request for a restriction on the disclosure of PHI by any Participant to the Payer Organizations and the Affirmative Consent is rejected if the patient indicates that he/she does not agree with the revocation or his/her prior request.

Note: As technology enhancements are made to accommodate such requests, this policy will be updated to reflect those enhancements.

Policy # P22: Request for Disclosure to Government Agencies for Health Oversight

I. Statement of Policy

With respect to access to PHI for health oversight 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.

II. Procedures

A. Any request for disclosure received from a government agency for health oversight will be submitted through HealtheConnections' Service Delivery Process for completion.

Policy # P23: Request for Disclosure to All Non-Health Oversight Government Agencies

I. Statement of Policy

With respect to all government agencies outside of health oversight (e.g., law enforcement), HealtheConnections is prohibited to disclose information except where required by law.

II. Procedures

A. If required by law, any request for disclosure received from a non-health oversight government agency will be submitted through HealtheConnections' Service Delivery Process for completion.

Policy # P24: Sanctions for Failure to Comply with the Policies and Procedures

I. Statement of Policy

HealtheConnections or its Participants shall implement sanctions and hold workforce members, agents, and contractors accountable for complying with the all the Policy and Procedures that are within this handbook.

II. Procedures

A. Any non-compliance of policy reported to the Participant or to HealtheConnections will be handled accordingly. For Breaches, refer to the procedures in Policy # P18: Breach Response and the sanctions outlined in Policy # P19: Sanctions for Breach.

B. Participants have an obligation to report any violation of the Policies and Procedures to the privacy officer of the affected entity as well as to HealtheConnections.

C. Such discipline measures may include, but not limited to, verbal and written warnings, re-training requirements, and termination of participation in the exchange.

D. HealtheConnections maintains a log of non-compliance sanctions imposed, including the date of non-compliance, type of non-compliance, and the imposed sanction.

E. HealtheConnections reports non-compliance to SHIN-NY Enterprise per Oversight and Enforcement policy reporting requirements.

Policy # P25: Provision of QE Data for Research Purposes

I. Statement of Policy

HealtheConnections will conduct a thorough evaluation of each research proposal before agreeing to provide data for research purposes. All research proposals will be required to have IRB approval and will be evaluated by the HeC Research Committee. All participants have agreed to allow their data to be used for research purposes in the HeC participation agreement.

II. Procedures

A. Once HeC receives a research request, the researcher will be asked to complete the HeC research request form.
B. The form will be used to evaluate the project and will go before the HeC Data Review Committee.
    1. De- Identified Data and Limited Data Sets
        i. If approved by the HeC Data Review Committee and proof of IRB approval is provided, de-identified data and limited data sets can be provided without patient consent based on SHIN-NY Privacy and Security Policy and Procedures §1.7.1 - §1.7.2
        ii. The researcher will be required to complete a Data Use Agreement that meets the requirements for use of de-identified data without patient consent, established in Policy # P02 'Exception to Affirmative Consent Requirement: De-Identified Data'.
    2. Use of PHI for Research
        i. Patient Recruitment
            1. If approved by the HeC Data Review Committee and proof of IRB approval is provided, PHI will be used by HeC to determine participants whose patients fall within the research criteria.
            2. HeC will then contact these participants with the researcher's information and the list of patients that qualify for the Research study and provide them with the Level 2 consent form that must be completed by the patient to allow access to patient PHI for research purposes.
            3. It is the responsibility of the researcher to gather the Level 2 consent forms from the participants and provide them to HeC for processing.
        ii. Retrospective Research
            1. HeC will provide PHI data for retrospective research as long as the following conditions are met:
                a. An IRB has approved the disclosure.
                b. The HeC Data Review Committee has approved the disclosure.
                c. the Data Supplier(s) that are the source of the Protected Health Information have agreed to allow for Disclosures of their Protected Health Information for purposes of Research.
    3. 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 Privacy and Security Policy and Procedures §1.7.5.

Policy # P26: Transmittals to Business Associates

I. Statement of Policy

HealtheConnections will allow transmittals to Business Associates of Participants as long as the appropriate agreements are in place and that the transmittal is in accordance with state and federal laws and the terms of the Business Associate Agreement. The Business Associate may not further disclose the PHI except where these Policies and Procedures allow for such disclosure.

II. Procedures

A. HeC receives a request to provide PHI to a Business Associate of a Participant.

B. The HeC employee to whom the request was made will consult with the HeC Policy Officer and will collect further information regarding the request.

C. Depending on the nature of the relationship between the requester and the intended recipient of the data, the appropriate HeC agreement(s) will be required to be completed between all parties involved in the exchange.

Policy # P27: Transmittals to Non-Participants

I. Statement of Policy

HealtheConnections may transmit Protected Health Information to non-participants only if the patient has granted Affirmative consent, provided that the Affirmative consent shall not be required if the transmittal is provided to a public health authority. The Affirmative Consent shall meet all the requirements of a Level 1 Consent provided that if the recipient is a life or disability insurer that is not a governmental entity then the form shall have been approved by the applicable department(s) of insurance.

A Transmittal may be made to a non-Participant on the basis of any Affirmative Consent that applies to such non-Participant, provided that none of the exceptions to the Affirmative Consent requirement set forth in SHIN-NY Privacy and Security Policies and Procedures § 1.2 other than Public Health Reporting and Access (§ 1.2.2) shall apply to Transmittals under this section.

II. Procedures

A. If HeC receives a request for a Transmittal to a Non-Participant, the CEO or Policy Officer will determine if the Transmittal will be allowed.
    1. Transmittals will only be allowed if the recipient is one of the following:
        a. A Covered Entity that does not operate in New York State, or a Business Associate of such Covered Entity.
        b. A Health Information Exchange Organization that does not operate in New York State.
        c. A public health authority, as defined at 45. C.F.R. § 164.501, that is not located in New York State.
        d. A health care facility that is operated by the United States Department of Veteran Affairs or the United States Department of Defense.
        e. A disability insurer or life insurer that has
            i. issued a disability or life insurance policy to the patient; received an application from the patient for such a policy; or
            ii. received a claim for benefits from the patient.
    2. Source of the Affirmative Consent must be confirmable by either HeC or the recipient of the Transmittal.
    3. HeC must be sure the Transmittal is delivered to the same individual or entity that is authorized in the patient's Affirmative Consent to receive the patient's PHI.
    4. HeC and recipient enter into an agreement with the recipient, such as a data use agreement.

Policy # P28: Cybersecurity

I. Statement of Policy

HealtheConnections has an Information Security Management Program with policies and procedures in place to identify, protect, detect, respond, and recover from security incidents, and is HITRUST certified, ensuring a superior level of security protection for our internal corporate environment and retail environment.

II. Procedures

A. All security concerns are mitigated, managed, tracked, monitored, assessed, identified, responded to, and controlled according to the policies and procedures that are required under an approved security and risk framework.

B. The HeC Security Officer will monitor the security environment of HeC and address concerns as they arise.

C. All branches of HeC will operate in a security-minded fashion, adhering to the approved HeC Security policies and procedures.

Appendix A: HealtheConnections Policies and Procedures Glossary

Access: 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: an organization of clinically integrated healthcare providers certified by the Commissioner of Health under N.Y. Public Health Law Article 29-E.

Affiliated Practitioner: (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: the consent of a patient obtained through the patient's execution of a Level 1 Consent Form; Level 2 Consent Form; or a consent that may be relied upon under the Patient Consent Transition Rules set forth in SHIN-NY Privacy and Security Policies and Procedures § 1.10.

*****All-In Consent (AIC):*** A Level 1 Consent, that at minimum, allows for disclosure of Protected Health Information to all current and future Participants who provide Treatment to a patient, regardless of which QE such Participants have contracted with. At the time of this writing, the final State Approved AIC (consent form) has not yet been issued.**

*****AIC Date**:** The date on which NYS DOH requires Participants to offer to patients the State Approved AIC Form. At the time of this writing, the AIC Date has not yet been determined.**

Audit Log: an electronic record of the disclosure of information via the SHIN-NY governed by the QE, 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.

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

***Breach*:** 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 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: 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 Policy #P02.

Business Associate Agreement: a written signed agreement meeting the HIPAA requirements of 45 CFR § 164.504(e).

Care Management: (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: 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: a committee that includes representatives of all QEs in the SHIN-NY, NYS DOH, and other relevant stakeholders 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 Applications: 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: 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.

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

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"): 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 Supplier: 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 governed by a QE (such as clinical laboratories and pharmacies). Government agencies, including Public Health Agencies, may be Data Suppliers.

De-Identified Data: 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: 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: 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: 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: 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: a person certified pursuant to the New York State Emergency Services Code at 10 N.Y.C.R.R. § 800.3(p) 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: 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: 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: an entity that contracts with a Health Home to provide services covered by New York's Medicaid Health Home program.

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

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

HIPAA Privacy Rule: the federal regulations at 45 CFR Part 160 and Subparts A and E of Part 164.

HIPAA Security Rule: the federal regulations at 45 CFR Part 160 and Subpart C of Part 164.

HITECH: the Health Information Technology for Economic and Clinical Health Act.

Independent Practice Association ("IPA"): 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: 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: 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.

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

Level 2 Consent: 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 C.

Level 1 Uses: Treatment, Quality Improvement, Care Management, Utilization Review, and Insurance Coverage Reviews. Note, Utilization Review has been added as a Level 1 Use only with respect to determinations of medical necessity. If a Utilization Review also includes payment decisions, a Level 2 Consent form must be utilized to gather consent.

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

Limited Data Set: 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.

Medical Examiner: 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.

Minimum Necessary: For any type of disclosure that a covered entity makes on a routine and recurring basis, that the covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, covered entities must develop and implement criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and review requests for disclosure on an individual basis in accordance with such criteria. A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when (a) making disclosures to public officials that are permitted under 45 CFR § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose, (b) if the information is requested by another covered entity (c) their business associates providing personal services, or (d) documentation or representations that comply with the applicable requirements of 45 CFR § 164.512(i) have been provided by an individual requesting the information for research purposes [45 CFR § 164.514(d)(3)].

The Minimum Necessary standard also applies to uses of protected health information [45 CFR § 164.514(d)(2)] and requests for protected health information [45 CFR § 164.514(d)(4)].

Minor Consent Information: Protected Health Information relating to medical treatment of a

minor for which the minor provided his or her own consent without a parent's or guardian's permission, as permitted by New York law for certain types of health services (e.g., reproductive health, HIV testing, mental health, or substance use treatment). This includes services consented to by an Emancipated Minor.

National Institute of Standards and Technology (NIST) Cybersecurity Framework: 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: the New York State Department of Health.

New York eHealth Collaborative ("NYeC"): the New York not-for-profit corporation organized for the purpose of (1) convening, educating, and engaging key constituencies, including health care and health IT leaders across New York State, QEs, CHITAs and other health IT initiatives. (2) developing common health IT policies and procedures, standards, technical requirements, and service requirements through a transparent governance process and (3) evaluating and establishing accountability measures for New York State's health IT strategy. NYeC is under contract to the NYS DOH to administer the Statewide Collaboration Process and through it develop Statewide Policy Guidance.

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: 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: a Provider Organization, Payer Organization, Practitioner, Independent Practice Association, Accountable Care Organization, Public Health Agency, Organ Procurement Organization, Health Home, Health Home Member, PPS Partner, PPS Lead Organization, PPS Centralized Entity, Social Services Program, a Community-Based Organization, 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 governed by a QE. For purposes hereof, "Participant" refers to each tax entity, whether an individual or an organization.

Participation Agreement: the agreement made by and between a QE and each of its Participants, which set 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: 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: 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.

Payment: 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.

Payer Organization: an insurance company, health maintenance organization, employee health benefit plan established under ERISA or any other entity that is legally authorized to provide health insurance coverage.

Practitioner: 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 he or she is practicing or a resident or student acting under the supervision of such a professional.

Personal Representative: 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.

PPS: a Performing Provider System that had received approval from NYS DOH to implement projects and receive funds under New York's Delivery System Reform Incentive Payment Program. Note: the DSRIP program ended March 31, 2020.

PPS Centralized Entity: an entity owned or controlled by one or more PPS Partners that has been engaged by a PPS to perform Care Management, Quality Improvement, or Insurance Coverage Reviews on behalf of the PPS.

PPS Lead Organization: an entity that has been approved by NYS DOH and CMS to serve as designated organization that has assumed all responsibilities associated with Delivery System Reform Incentive Payment ("DSRIP") program per their project application and DSRIP award.

PPS Partner: means a person or entity that is listed as a PPS Partner in the DSRIP Network Tool maintained by NYS DOH.

Protected Health Information (PHI): 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: an entity such as a hospital, nursing home, home health agency or professional corporation legally authorized to provide health care services.

Public Health Agency: 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 governed by a QE.

QE Research Committee: 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 (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 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 (3) does not have any member participating in a review of any project in which the member has a conflict of interest.

Qualified Health IT Entity ("QE"): 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: 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 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: a system, queried only by Authorized Users, that provides an electronic means for identifying and locating a patient's medical records across Data Suppliers.

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

Retrospective Research: 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 (Regional Health Information Organization): a not-for-profit corporation that (i) receives funding and was designated as a RHIO under Phase 5 of the Healthcare Efficiency and Affordability Law for New Yorkers or (ii) is currently designated as a QE (Qualified Entity) by the NYS DOH and agrees in writing with NYeC to follow the Statewide Policy Guidance applicable to QEs as developed through the SCP.

RHIO Administrator: point of contact for any communication with the QE on any of the policies and procedures within this handbook.

Sensitive Health Information: 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 (Statewide Health Information Network of New York): 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 governed by 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 Privacy and Security Policies and Procedures (SHIN-NY Policy): Statewide guidance [consistent with 10 N.Y.C.R.R. § 300.3(b)(1)] governing secure health information

exchange through the Statewide Health Information Network for New York (SHIN-NY). HealtheConnections and all Participants are required to adhere to this guidance. This guidance, as may be updated periodically, is available here: https://www.health.ny.gov/technology/regulations/shin-ny/docs/privacy_and_security_policies.pdf

Social Services Program: 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: 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 Approved AIC***: The All-In Consent form approved and issued by NYS DOH. At the time of this writing, the State Approved AIC has not yet been issued.**

Statewide Collaborative Process (SCP): the open, transparent process to which multiple stakeholders contribute, administered by NYeC, to develop Statewide Policy Guidance, to be adopted and complied with by all QEs and their Participants.

Statewide Policy Guidance: the common policies and procedures, standards, technical requirements, and service requirements developed through the SCP.

Telehealth: 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: a QE's transmission 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: 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: 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: 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.

Appendix B: Resources

Health Advancement Collaborative of CNY/ HealtheConnections – www.healtheconnections.org

New York State Department of Health – www.health.ny.gov

SHIN-NY Privacy and Security Policies and Procedures (SHIN-NY Policy) – https://www.health.ny.gov/technology/regulations/shin-ny/docs/privacy_and_security_policies.pdf

New York State eHealth Collaborative (NYeC) – www.nyehealth.org

New York State Office of Attorney General (Breach Law) - http://www.ag.ny.gov

New York State Office of Cyber Security and Critical Infrastructure Laws (Breach Law) http://www.its.ny.gov/eiso

U.S. Department of Health and Human Services: Health Information Technology - http://www.healthit.gov

HITECH Breach Notification Interim Final Rule – https://www.govinfo.gov/content/pkg/FR-2009-08-24/pdf/E9-20169.pdf

Appendix C: Model Level 1 and Level 2 Approved Consent Forms

See approved model Level 1 and Level 2 Consent Forms at NYS DOH website at https://www.health.ny.gov/technology/regulations/shin-ny/docs/privacy_and_security_policies.pdf for the following:

- Model Level 1 Consent Form for Providers without Emergency Services
- Model Level 1 Consent Form for Providers with Emergency Services
- Model Level 1 All-in Consent (State Approved AIC) **Not yet issued**
- Model Level 2 Payer Consent Form for Payment
- Model Level 2 Research Consent Form
- Model Level 2 Supplemental Security Income (SSI) Application Consent Form

Participant-customized consent forms for HealtheConnections' Participants will be provided.