



# **HealthConnections Privacy and Security Policy and Procedures Handbook**

**February 22, 2017**

## **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 in the Central New York area (“HealtheConnections”) 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, Version 3.3*. 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 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

<b>Policy # P01: Compliance with Laws and Policies</b> .....	4
<b>Policy # P02: Patient Consent - Level 1</b> .....	5
<b>Policy # P03: Patient Consent - Level 2</b> .....	11
<b>Policy # P04: Authorized User Roles and Management</b> .....	12
<b>Policy # P05: Certification of Authorized Users</b> .....	13
<b>Policy # P06: Authentication Level and Management</b> .....	14
<b>Policy # P07: Business Associate Agreements</b> .....	15
<b>Policy # P08: Minimum Necessary Access – Other Than Use For Treatment</b> .....	16
<b>Policy # P09: Access Policies to HIE</b> .....	17
<b>Policy # P10: Termination of Access</b> .....	18
<b>Policy # P11: Amendment of Data</b> .....	19
<b>Policy # P12: Audit Logs</b> .....	20
<b>Policy # P13: Request for Audit Logs by a Participant</b> .....	21
<b>Policy # P14: Request for Audit Logs by a Patient</b> .....	22
<b>Policy # P15: Periodic Audits</b> .....	23
<b>Policy # P16: Public Availability of Audits</b> .....	24
<b>Policy # P17: Privacy Complaints and Concerns</b> .....	25
<b>Policy # P18: Breach Response</b> .....	26
<b>Policy # P19: Sanctions for Breach</b> .....	29
<b>Policy # P20: Patient Engagement and Access</b> .....	30
<b>Policy # P21: Request for Disclosure Restriction to Payer Organizations</b> .....	31
<b>Policy # P22: Request for Disclosure to Government Agencies for Health Oversight</b> .....	32
<b>Policy # P23: Request for Disclosure to All Non-Health Oversight Government Agencies</b> .....	33
<b>Policy # P24: Sanctions for Failure to Comply with the Policies and Procedures</b> .....	34
<b>Appendix A: HealthConnections Policies and Procedures Glossary</b> .....	35
<b>Appendix B: Resources</b> .....	40
<b>Appendix C: Model Level 1 Approved Consent Forms</b> .....	41

## **Policy # P01: Compliance with Laws and Policies**

### **I. Statement of Policy**

HealthConnections Participants must comply with all applicable federal, state and local laws, rules and regulations and Policies and Procedures in order to provide essential privacy protections for patients, and must implement appropriate internal policies and procedures for compliance therewith.

### **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. 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.
2. 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.

#### **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 HealthConnections (the “RHIO Administrator”).

#### **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.

<b>Policy # P02: Patient Consent - Level 1</b>
--

### **I. Statement of Policy**

New York State law requires that hospitals, physicians and other health care providers and payers obtain the consent of patients or their personal representatives before disclosing PHI for non-emergency treatment. Therefore, affirmative consent must be obtained from the patient or personal representative before each Participant can access a patient's health information. From this point forward any reference to the patient consent also includes consent obtained by a patient's personal representative.

### **II. Procedure**

#### **A. General Considerations**

1. Unless an exception applies (see Section II-D through J), Affirmative Consent of the patient must be obtained by each Participant before a patient's health information is accessed using a state approved consent form available through HealtheConnections.
2. An Affirmative Consent obtained by a Participant shall apply to 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 his or her 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.
3. At a Participant's option, 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. 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. Access to the Multi-Provider approved consent form can be found in Appendix C.
4. 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.

5. 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.
6. If a patient consents, the information accessible through the exchange will include the following sensitive information:
  - 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 abuse information
7. All patient consents must be obtained using the HealtheConnections Patient Consent Form. 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.
8. Patients may change their consent at any time by completing a new patient consent form.
9. 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". Any non-physician authorized user must indicate on the "break the glass" screen that s/he is accessing the patient's records under direction of a physician.
10. 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 ("HIE-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.
11. 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.
12. Providers/Payers must not condition treatment/coverage on the patient's willingness to consent to the access of their health information through HealtheConnections.
13. Consent may be obtained electronically provided that there is an electronic signature that meets the requirements of the federal E-SIGN statute, 15 U.S.C. § 7001 et seq., or any other applicable New York State or federal laws or regulations.
14. A patient's consent is not time-limited.
15. 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.
16. 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 on 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 treating practitioner to receive information from or send information to an identified source. 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 practitioner who ordered the test.
2. Participant practitioners 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 that of the two exchanging providers. Therefore, affirmative patient consent is not needed for one-to-one exchange of health information. However, if a

patient requests limitations on the disclosure of his/her information electronically through the health information exchange, the practitioner may comply with this request.

4. NYS laws requiring written consent for release of sensitive information as identified in Section II-A-6 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: 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) to access a patient's Protected Health Information through the health information exchange and the Practitioner may 'Break the Glass' if the following conditions are met:
  - a) Treatment may be provided to the patient without informed consent as provided in Public Health Law Section 2504(4), i.e., in the Practitioner's judgment an emergency condition exists and 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 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 is affiliated.
  - d) The Practitioner attests that all of the foregoing conditions have been satisfied.
  - e) The right to 'Break the Glass' terminates with the completion of an emergency treatment. If the practitioner seeks to access the patient's health information after the emergency has ended, s/he must comply with patient consent requirements.
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-1 (a-c) are met.
3. HealtheConnections will maintain a record of any 'Break the Glass' access.

#### **G. Exception to Affirmative Consent Requirement: De-Identified Data**

1. Affirmative Consent shall not be required for a Participant to access De-Identified Data through the exchange for the following purposes:
  - a) Research approved by an Institutional Review Board or Privacy Board organized and operating in accordance with 45 C.F.R. § 164;
  - b) Evaluation and improvement of RHIO operations, including analyses performed by the RHIO, government agencies or their contractors; or
  - c) Any purpose for which the RHIO, Participant, or government agency may access Protected Health Information under these Policies and Procedures.



2. HealtheConnections may use PHI to create and validate the accuracy of De-Identified Data that is used in accordance with G-1 (a-c).
3. All other uses of De-Identified Data shall require Affirmative Consent. Examples include Participant fundraising and other marketing purposes.
  - a) Participants shall not condition a patient's participation in the exchange on the patient's decision to consent or deny access to De-Identified Data for purposes other than those set forth in Section G-1.
4. Participants and business associates must comply with standards for the de-identification of data set forth in 45 C.F.R. § 164.514.
5. Participants are subject to adequate restrictions on the re-identification of De-identified data.
6. Participants should have and follow their own internal policies when determining access to de-identified information and for what purpose.

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

#### **I. 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 RHIO operations.
2. This is limited to the minimum necessary information required to accomplish the intended purpose of the use or disclosure.

#### **J. 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.

#### **K. Exception to Affirmative Consent Requirement: Organ Procurement Organization Access**

1. A RHIO 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 RHIO to access the patient's PHI shall not prevent or otherwise restrict an Organ Procurement Organization from accessing the patient's PHI through a RHIO.

## 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.

### **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**

It is required that all HealthConnections' Participants identify and maintain each of their Authorized User Roles. The following are the roles associated with the health information exchange:

- a. Break the Glass Practitioner
- b. Break the Glass Non-practitioner
- c. Practitioner with access to clinical and non-clinical information
- d. Non-practitioner with access to clinical and non-clinical information
- e. Non-practitioner with access to non-clinical information
- f. QE administrator with access to non-clinical information
- g. QE administrator with Public Health access
- h. Public Health
- i. Administrator

### **II. Procedures**

- A. The Participant's RHIO Administrator(s) will identify and manage their authorized users' roles and communicate the same to HealthConnections via the Authorized User Certification and Application form.
- B. HealthConnections will set up the user accounts per the approved Authorized User Certification and Application 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 Participants' designated Authorized Users, prior to becoming an Authorized User, 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, a Level 2 standard for authentication of each Authorized User. This requires proper identification prior to access and unique passwords to enter the system.

### **II. Procedures**

- A. HealthConnections representative will meet with the Participant's designated RHIO Administrator prior to implementing RHIO processes at the participating organization.
- B. Upon proper identification of the Authorized User, the Participant's RHIO Administrators can request access to the HIE for the Authorized User.

## **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**

HealthConnections' 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.

#### **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**

HealthConnections 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. HealthConnections 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 for a set period of time after which they can attempt to log back in. The user may also contact HealthConnections Support to re-set their password. After HealthConnections Support re-sets the password, an email is sent to the RHIO Administrator and the Authorized User, indicating that this action has taken place.
- 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**

HealthConnections 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. All requests for amendments and/or corrections must go through the data source Participant, not through HealthConnections.
- B. 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.

## Policy # P12: Audit Logs

### I. Statement of Policy

It is required that the HealthConnections 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.
- b. The identity of the Authorized User accessing 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).
- e. Date and time of access.
- f. The source of the Protected Health Information (i.e., the identity of the Participant from whose records the accessed 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.

## **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 6 year 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 an 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 Logs by a Patient

### **I. Statement of Policy**

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

- a. The name and role of each Authorized User who accessed a patient's Protected Health Information in the prior 6 year period.
- b. The Participant through which such Authorized User accessed Protected Health Information.
- c. The time and date of such access.
- d. 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. Patients will contact HealtheConnections for such a request.
- C. Patients may request one free audit of disclosures every 12 months. Should the patient request an additional audit during any 12 month period, a fee will 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.
- D. The following types of disclosures are exempt from the accounting requirements set forth in this policy:
  1. Disclosures for treatment, payment , and health care operations
  2. Disclosures to the individual of their own PHI
  3. Disclosures made pursuant to an authorization from the individual
  4. Disclosures that are incident to a permitted use and disclosure
  5. Disclosures for the patient directory or to the persons involved in the individual's care or notification purposes.
  6. Disclosures made prior to April 14, 2003
- E. The Participant will be notified of such patient requests, unless it is determined by HealtheConnections that such notification will jeopardize the privacy and security of the patient.

## Policy # P15: Periodic Audits

### I. Statement of Policy

It is required that HealtheConnections and each of its Participants conduct at least a yearly audit. The following information must be audited:

- a. Consents on file
- b. Authorized Users who access Protected Health Information do so for authorized purposes
- c. Requirements were met under Break the Glass

### II. Procedures

- A. Participants will be required to provide proof to HealtheConnections that an Affirmative Consent form is on file for a list of patients on a statistically significant sample size that will be produced by HealtheConnections.
- B. HealtheConnections will conduct the Authorized User access audits and the Break the Glass audits.
- C. HealtheConnections has the authority to conduct random consent audits on its Participants.

## **Policy # P16: Public Availability of Audits**

### **I. Statement of Policy**

It is required that HealtheConnections makes results of the audits available on the website no more than 30 days after the completion of an audit.

### **II. Procedures**

A. HealtheConnections will post information about audit results on the HealtheConnections website.



## Policy # P17: Privacy Complaints and Concerns

### **I. Statement of Policy**

Each HealthConnections 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 HealthConnections 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 HealthConnections 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. HealthConnections Operations Support will archive the summaries of the complaints/reports for later reporting and discussion.
- E. In the event that a Participant or HealthConnections associate feels there is a complaint or concern that suggests HealthConnections' investigation of the complaint/concern is a conflict of interest, it will be reported to the President of the HAC-CNY Board.

## Policy # P18: Breach Response

### I. Statement of Policy

HealthConnections 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 HealthConnections
  1. HealthConnections 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 HealthConnections 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 HealthConnections 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 HealthConnections Operations Support 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 of a breach of information systems by HealthConnections associates, the following process will be followed, unless otherwise stated in their Business Associate Agreements:
  1. HealthConnections 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) The Participant will perform a risk analysis to determine the financial, reputational, or other harm to the patient potentially caused by the breach.
    - d) The participant will send letters within 60 days that the breach became known by HealthConnections 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.
    - 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 HAC-CNY 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 President of the HAC-CNY 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 know 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.
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 of the breach.
6. Notification should include, to the extent possible, the following:
  - b) A brief description of what happened, including the date of the breach and the date of the discovery, if known.
  - c) A description of the types of unsecured protected health information that were involved in the breach (i.e. name, SS#, address, etc).
  - d) The steps individuals should take to protect themselves from potential harm resulting from breach.
  - e) A brief description of what the Participant involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

- f) 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 not limited to:
  - a) Re-training on the policy and procedures
  - b) Verbal or written warnings
  - c) Suspension of access for an Authorized User
  - d) Termination of access for an Authorized User
  - e) Suspension of access for all Participants Authorized Users
  - f) Termination of Participation Agreement

#### **C. Other Sanctions**

1. In the event that a breach is reported to the President of the HAC-CNY 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 HAC-CNY 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.

### **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 HITEC, HealthConnections 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 RHIO 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.

<p><b>Policy # P22: Request for Disclosure to Government Agencies for Health Oversight</b></p>
--

**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.

**II. Procedures**

A. Unless required by law, HealtheConnections will not disclose any PHI requested by health oversight agencies.



**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 (i.e., law enforcement), HealtheConnections is prohibited to disclose information except where required by law.

**II. Procedures**

A. Unless required by law, HealtheConnections will decline to give access to any PHI within the exchange to government agencies outside health oversight.

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

### **I. Statement of Policy**

Each HealthConnections' Participant 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 breach of confidentiality reported to the Participant or to HealthConnections will be handled according to the procedures in Policy # P18: Breach Response and the sanctions outlined in Policy # P20: 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 HealthConnections.

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

## Appendix A: HealthConnections Policies and Procedures Glossary

**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 or a Level 2 Consent Form.

**Audit Log:** an electronic record of the access of information via the health information exchange, such as queries made by Authorized Users, type of information accessed, information flows between the RHIO and Participants, and date and time markers for those activities.

**Authorized User:** an individual who has been authorized by a Participant or a RHIO to access patient information via health information exchange in accordance with the 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. For purposes of this definition, "compromises the security or privacy of the Protected Health Information" means poses a significant risk of financial, reputational, or other harm to the individual. 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 RHIO 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 RHIO or Participant to another person authorized to access Protected Health Information at the same RHIO 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 RHIO 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 or (iv) supporting a patient in following a plan of medical care. Care Management does not include utilization review or other activities carried out by a Payer Organization to determine whether coverage should be extended or payment should be made for a health care service.

**Data Supplier:** an individual or entity that supplies Protected Health Information to or through a RHIO. Data Suppliers include both Participants and entities that supply but do not access

Protected Health Information via health information exchange (such as clinical laboratories and pharmacies).

**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 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.

**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.

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

**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.

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

**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 Form:** a consent form used for treatment, quality improvement, care management, and insurance coverage reviews.

**Level 2 Consent Form:** a consent form for any uses of Protected Health Information other than Level 1 Uses, including but not limited to payment, research, and marketing.

**Level 1 Uses:** Treatment, Quality Improvement, Care Management, and Insurance Coverage Reviews.

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

**Marketing:** has the meaning ascribed to this term under the HIPAA Privacy Rule as amended by Section 13406 of HITECH.

**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 abuse treatment). This includes services consented to by Emancipated Minors.

**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, RHIOs, 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:** a disclosure of Protected Health Information by one of the patient's providers to one or more other providers treating the patient with the patient's knowledge and implicit or explicit consent where no records other than those of the Participants jointly providing health care services to the patient are exchanged. A One-to-One Exchange is an electronic transfer of information that is understood and predictable to a patient, because it mirrors a paper-based exchange, such as a referral to a specialist, a discharge summary sent to where the patient is transferred or lab results sent to the Practitioner who ordered them.

**Participant:** a Provider Organization, Payer Organization, or Practitioner that has directly or indirectly entered into a Participation Agreement with a RHIO and accesses Protected Health Information via the health information exchange. For purposes hereof, "Participant" refers to each tax entity, whether an individual or an organization.

**Participation Agreement:** the agreement made by and between a RHIO and each of its Participants, which set forth the terms and conditions governing the operation of the RHIO and the rights and responsibilities of the Participants and the RHIO with respect to the RHIO.

**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 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.

**Privacy and Security White Paper:** the final draft of the policy paper, as approved by each of the NYeC Board of Directors and the NYS DOH, entitled "Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York State."

**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 in New York State.

**Qualified Entity:** an entity that has been certified by NYS to manage and govern services defined by the State Health Information Network of New York (SHIN-NY).

**Quality Improvement:** conducting quality measurement, assessment and improvement, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health and reducing health care costs, evaluating Practitioner and provider performance, clinical decision support tools, evidence-based clinical protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives and related functions. Care management by payers may include (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 or (iv) supporting a patient in following a plan of medical care; provided, however, that no such activity may include utilization review or other tasks designed to determine whether a payer should cover or make payment for a health care service.

**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.

**RHIO:** 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 otherwise designated as a RHIO by the NYS DOH or (iii) an organization that meets the definition of RHIO as set forth in the HEAL 5 Request for Grant Applications and agrees in writing with NYeC to follow the Statewide Policy Guidance applicable to RHIOs as developed through the SCP.

**RHIO Administrators:** point of contact for any communication with the RHIO 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 abuse, reproductive health, sexually-transmitted disease, and genetic testing information.

**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 RHIOs and their Participants.

**Statewide Health Information Network of New York (SHIN-NY):** a “network of networks” overseen by NYS DOH and governed by RHIOs, which enables patient health information to be exchanged in real time among disparate clinicians, other authorized entities, and patients, while ensuring security, privacy and other protections.

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

**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.

## Appendix B: Resources

eHealth for New York – [www.ehealth4ny.org](http://www.ehealth4ny.org)

Health Advancement Collaborative of CNY – [www.healthconnections.org](http://www.healthconnections.org)

HealthConnections RHIO Central New York – [www.healthconnections.org](http://www.healthconnections.org)

New York State Department of Health – [www.nyhealth.gov](http://www.nyhealth.gov)

New York State eHealth Collaborative – [www.nyehealth.org](http://www.nyehealth.org)

New York State Office of Attorney General (Breach Law) -  
[http://www.oag.state.ny.us/bureaus/consumer\\_frauds/tips/id\\_theft\\_law.html](http://www.oag.state.ny.us/bureaus/consumer_frauds/tips/id_theft_law.html)

New York State Office of Cyber Security and Critical Infrastructure Laws (Breach Law)  
<http://www.cscic.state.ny.us/security/securitybreach/>

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

HITECH Breach Notification Interim Final Rule -  
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/breachnotificationifr.html>



## **Appendix C: Model Level 1 Approved Consent Forms**

See approved model Level 1 Consent Forms at NYeC website at [www.nyehealth.org/SCP-policies](http://www.nyehealth.org/SCP-policies) for the following:

- ◆ Level One Model Consent Form for Providers without Emergency Services
- ◆ Level One Model Consent Form for Providers with Emergency Services