Introduction

This document, the Privacy and Security Policies and Procedures for Qualified Entities and their Participants (the “Policies and Procedures”), sets forth the privacy and security-related policies governing interoperable health information exchange through the Statewide Health Information Network for New York (the “SHIN-NY”). Through the adoption of comprehensive, standardized policies and procedures governing privacy and security, New York State aims to ensure trusted health information exchange through the SHIN-NY that will improve health care delivery and health outcomes for all New Yorkers.

The New York State Department of Health (“NYS DOH”), along with key stakeholders, participated in the development of the Policies and Procedures through the Statewide Collaboration Process described below. It is the opinion of the NYS DOH that the Policies and Procedures are compliant with state and federal laws.

The Statewide Collaboration Process

New York State’s governance structure for health information technology and exchange is characterized by collaborative statewide leadership by the New York eHealth Collaborative (“NYeC”) and NYS DOH. Under the guidance of these two entities, New York State has developed an open, transparent, collaborative, multi-stakeholder process for developing policies, standards, protocols, operational guidance and technical approaches for health information exchange through the SHIN-NY. This collaborative process is known as the Statewide Collaboration Process (the “SCP”).

How the Statewide Collaboration Process Works

In keeping with the goals of stakeholder involvement through an open and transparent process, NYeC, in collaboration with NYS DOH, established several stakeholder groups to provide feedback on the development of the SHIN-NY, including the SHIN-NY Business and Operations Committee (the “BOC”) and the SHIN-NY Policy Committee. These Committees are committees of the NYeC Board and are representative of key stakeholder constituencies across the state. In addition to these committees, consumer and provider focus group forums help inform SHIN-NY product and services development. NYeC also seeks public comment on SHIN-NY Policy Standards, program initiatives, and service plans.

SHIN-NY Policy Standards

These Policies and Procedures provide a common and consistent framework for the exchange of patient health information through the SHIN-NY. They are part of the SHIN-NY Policy Standards, which is the set of policies and procedures, including technical standards and SHIN-NY services and products, developed through the SCP and adopted by NYS DOH as provided in 10 N.Y.C.R.R. Section 300.3.

Process for Amending the Policies and Procedures
The Statewide Collaboration Process: Policies and Procedures

The Policies and Procedures are subject to a regular amendment process that is determined by the SHIN-NY Policy Committee. Proposed changes are solicited during an open comment period and are evaluated and implemented, as appropriate, through the SCP.

Who Must Comply with the Policies and Procedures

Qualified Health IT Entities (“QEs”) and their Participants must comply with the Policies and Procedures and other SHIN-NY Policy Standards. A QE must accept the performance of any other QE that meets the requirements of the Policies and Procedures and may not require additional performance above the level required in the Policies and Procedures or impose any other requirement that would impede statewide interoperability and exchange of health information. QEs must require their Participants to comply with the Policies and Procedures through the terms of the Participant Agreement that a QE enters into with a Participant.

The Policies and Procedures Operational Guide Best Practices

The Operational Guide Best Practices (the “Guide”) serves as a companion document to the Policies and Procedures. However, unlike the Policies and Procedures, it is not incorporated by reference into the SHIN-NY regulations. The Guide defines best practice approaches for QE implementation of the policies set forth in the Policies and Procedures. QEs are not required to follow the best practices set forth in the Guide but they may consult the Guide on a voluntary basis.

Definitions:

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

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

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

Affirmative Consent means the consent of a patient obtained through the patient’s execution of (i) a Level 1 Consent; (ii) a Level 2 Consent; (iii) a consent mechanism approved by NYS DOH as an alternative to a Level 1 Consent or a Level 2 Consent under Section 1.3; or (iv) a consent that may be relied upon under the Patient Consent Transition Rules set forth in Section 1.8.2.

Approved Consent means an Affirmative Consent other than a consent relied upon by a Participant under the Patient Consent Transition Rules set forth in Section 1.8.2.

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

Authorized User means 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 the Policies and Procedures.
The Statewide Collaboration Process:  
Policies and Procedures

Breach means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the Protected Health Information. An acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Participant or QE can demonstrate that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the Protected Health Information or to whom the disclosure was made; (ii) 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 means the ability of an Authorized User to access a patient’s Protected Health Information without obtaining an Affirmative Consent in accordance with the provisions of Section 1.2.3.

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

Care Management means (i) assisting a patient in obtaining appropriate medical care, (ii) improving the quality of health care services provided to a patient, (iii) coordinating the provision of multiple health care services to a patient 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.

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

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

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.

Data Supplier means an individual or entity that supplies Protected Health Information to or through a QE. Data Suppliers include both Participants and entities that supply but do not access Protected Health Information via the SHIN-NY governed by a QE (such as clinical laboratories and pharmacies).
De-Identified Data means data that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Data may be considered de-identified only if it satisfies the requirements of 45 C.F.R. § 164.514(b).

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

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

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

Health Home means an entity that is enrolled in New York’s Medicaid Health Home program and that receives Medicaid reimbursement for providing care management services to participating enrollees.

Health Home Member means an entity that contracts with a Health Home to provide services covered by New York’s Medicaid Health Home program.

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

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

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

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

Independent Practice Association (“IPA”) means an entity that is certified as an independent practice association under 10 N.Y.C.R.R. § 98-1.5(b)(6)(vii).

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

Level 1 Consent means a consent permitting access to Protected Health Information for Level 1 Uses in the form attached hereto as Appendix A.

Level 2 Consent means a consent permitting access to Protected Health Information for a Level 2 Use in the form attached hereto as Appendix B.

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

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

Marketing has the meaning ascribed to this term under the HIPAA Privacy Rule as amended by Section 13406 of HITECH.
The Statewide Collaboration Process:  
Policies and Procedures

Minor Consent Information means 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 or other applicable laws for certain types of health services (e.g., reproductive health, HIV testing, mental health or substance abuse treatment) or services consented to by an Emancipated Minor.

NYS DOH means the New York State Department of Health.

New York eHealth Collaborative ("NYeC") means 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, 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 SCP and through it develop SHIN-NY Policy Standards.

One-to-One Exchange means a disclosure of Protected Health Information by one of the patient’s providers or other Participants to one or more other Participants either treating the patient or performing Quality Improvement and/or Care Management activities for such 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, lab results sent to the Practitioner who ordered them or clinical information sent from a hospital to the patient’s health plan for Quality Improvement or Care Management/coordination activities for such patient.

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

Participant means a Provider Organization, Payer Organization, Practitioner, Independent Practice Association, Accountable Care Organization, Public Health Agency, Organ Procurement Organization, Health Home or Health Home Member 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.

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

Patient Care Alert means an electronic message about a development in a patient’s medical care, such as an emergency room or inpatient hospital admission or discharge, a scheduled outpatient surgery or other procedure, or similar event, which is derived from information maintained by a QE and is sent 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 Consent Transition Rules means the rules set forth in Section 1.8.

Payment means the activities undertaken by (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or (ii) a health care provider or
The Statewide Collaboration Process:
Policies and Procedures

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

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

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

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

**Public Health Agency** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, 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.

**Qualified Health IT Entity (“QE”)** means a not-for-profit entity that has been certified as a QE under 10 N.Y.C.R.R. Section 300.4 and has executed a contract with the State Designated Entity under 10 N.Y.C.R.R. Section 300.7 pursuant to which it has agreed to be bound by SHIN-NY Policy Standards.

**Quality Improvement** means activities designed to improve processes and outcomes related to the provision of health care services. Quality Improvement activities include but are not limited to outcome evaluations; development of clinical guidelines; population based activities relating to improving health or reducing health care costs; clinical protocol development and decision support tools; case management and care coordination; reviewing the competence or qualifications of health care providers, but shall not include Research. The use or disclosure of Protected Health Information for quality improvement activities may be permitted provided the accessing and disclosing entities have or had a relationship with the individual who is the subject of the Protected Health Information.

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

**Research** means a systematic investigation, including research development, testing and evaluation designated to develop or contribute to generalizable knowledge, including clinical trials.
The Statewide Collaboration Process: Policies and Procedures

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

SHIN-NY means a set of agreements (and the transactions, relations and data that are created by and through such set of agreements) between the NYS DOH, the State Designated Entity, QEs and Participants to make possible the exchange of clinical information among Participants for authorized purposes to improve the quality, coordination and efficiency of patient care, reduce medical errors and carry out public health and health oversight activities, while protecting privacy and security. Pursuant to such agreements, the State Designated Entity, the QEs and the Participants agree to be bound by policy and technical requirements in SHIN-NY Policy Standards that has been created through the Statewide Collaboration Process.

Statewide Collaborative Process (“SCP”) means an open, transparent process to which multiple SHIN-NY stakeholders contribute, that is administered by the State Designated Entity for the development of SHIN-NY Policy Standards as provided in 10 N.Y.C.R.R. Section 300.3.

State Designated Entity means the single entity that: (1) has been designated by the Governor as eligible to receive from the federal government state grants to promote health information technology and conforms to federal requirements to receive such awards, or that has been certified by the Commissioner of Health as meeting the requirements of 10 N.Y.C.R.R. Part 300; (2) is a not-for-profit entity that includes on its board of directors representation from a broad range of SHIN-NY stakeholders; (3) demonstrates that its principal purpose is to serve the people of the State of New York by using information technology to create and maintain the SHIN-NY; and (4) adopts nondiscrimination and conflict of interest policies that demonstrate a commitment to open, fair, and nondiscriminatory participation by SHIN-NY stakeholders.

SHIN-NY Policy Standards means the set of policies and procedures, including technical standards and SHIN-NY services and products, that are developed through the Statewide Collaboration Process and adopted by NYS DOH as provided in 10 N.Y.C.R.R. Section 300.3, including the SHIN-NY Policy Standards incorporated by reference in subdivision (c) of that section.

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

Unsecured Protected Health Information means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services in guidance issued under section 13402(h)(2) of HITECH.
The Statewide Collaboration Process: Policies and Procedures

SECTION 1: CONSENT

Purpose/Principles

The purpose of these Policies and Procedures is to ensure the privacy and security of patients’ Protected Health Information while facilitating the sharing of such information to provide better quality health care.

Current laws governing health information exchange and the resulting business practices were developed in the context of a paper-based health care environment where decisions regarding what, how and to whom to communicate were generally made on a one-to-one basis by clinicians and their patients. Current laws attempt to serve patients’ privacy interests by restricting what can and cannot be shared, and the terms on which sharing takes place. Human judgment and personal relationships play a major role, as clinicians attempt to act as guardians of their patients’ information.

Moving from a paper to an electronic health system changes the information-sharing dynamic. An interoperable health information system facilitates a many-to-many relationship, enabling different information technology systems and software applications to exchange information accurately, effectively and consistently. This offers new opportunities to promote patient access to and control over health care information, as well as to facilitate the safety, quality and efficiency of health care.

Requiring patients to consent to the exchange of their information via the SHIN-NY governed by a QE ensures that they know how their information will be shared and used among QE Participants. It also lets patients decide whether to allow their information to be shared and used in this manner. The Policies and Procedures set forth in this Section 1 prescribe minimum State requirements for obtaining patient consent to exchange health information via the SHIN-NY governed by a QE.

Patient consent is an important element in achieving informed and trusted interoperable health information exchange as well as satisfying New York laws and regulations. It is important to observe, however, that consent policies alone are not enough and that such policies must be accompanied by privacy and security protections relating to authorization, authentication, access, audit and enforcement to earn consumer trust and enable successful health information exchange. Furthermore, it is essential that patient consent be implemented in conjunction with a robust consumer education program to ensure the consent decision is well informed.

Policies and Procedures

1.1 Requirement to Obtain Affirmative Consent. Except as set forth in Section 1.2, a Participant shall not access a patient’s Protected Health Information via the SHIN-NY governed by a QE unless the patient has provided an Affirmative Consent authorizing the Participant to access such Protected Health Information. An Affirmative Consent may be executed by an electronic signature as permitted by Section 1.7.5.

1.2 Exceptions to Affirmative Consent Requirement. Notwithstanding anything to the contrary set forth in this Section 1, Affirmative Consent shall not be required under the circumstances set forth in this Section 1.2.

1.2.1 One-to-One Exchanges. Affirmative Consent shall not be required for a Participant to access a patient’s Protected Health Information via the SHIN-NY governed by a QE from another Participant in a One-to-One Exchange provided the Participants comply with
The Statewide Collaboration Process: Policies and Procedures

existing federal and state laws and regulations requiring patient consent for the disclosure and re-disclosure of information by health care providers.1

1.2.2 Public Health Reporting and Access.

a. A Public Health Agency may access Protected Health Information through a QE’s clinical viewer or portal for the following public health purposes without Affirmative Consent: [BOC 9/23/2013 Request #1]

i. To investigate suspected or confirmed cases of communicable disease (pursuant to 10 N.Y.C.R.R. Part 2);

ii. To ascertain sources of infection (pursuant to 10 N.Y.C.R.R. Part 2);

iii. To conduct investigations to assist in reducing morbidity and mortality (pursuant to 10 N.Y.C.R.R. Part 2);

iv. To investigate suspected or confirmed cases of lead poisoning (pursuant to 10 N.Y.C.R.R. § 67-2.3); or

v. For other public health purposes authorized by law and approved through the Statewide Collaboration Process.

b. A patient's denial of consent for all Participants in a QE to access the patient’s Protected Health Information under Section 1.7.6 shall not prevent or otherwise restrict a Public Health Agency from accessing the patient's Protected Health Information through a QE for the purposes set forth in Section 1.2.2(a)(i)-(v).

c. If a Data Supplier or Participant is permitted to disclose Protected Health Information to a government agency for purposes of public health reporting, including monitoring disease trends, conducting outbreak investigations, responding to public health emergencies, assessing the comparative effectiveness of medical treatments (including pharmaceuticals), conducting adverse drug event reporting, and informing new payment reforms, without patient consent under applicable state and federal laws and regulations, a QE may make that disclosure on behalf of the Data Supplier or Participant without Affirmative Consent.

1.2.3 Breaking the Glass When Treating a Patient with an Emergency Condition.

a. Affirmative Consent shall not be required for (i) a Practitioner; (ii) an Authorized User acting under the direction of a Practitioner; or (iii) an Advanced Emergency Medical Technician to access Protected Health Information via the SHIN-NY

1 New York law currently requires patient consent for the disclosure of information by health care providers for non-emergency treatment purposes. For general medical information, this consent may be explicit or implicit, written or oral, depending on the circumstances. The disclosure of certain types of sensitive health information may require a specific written consent. Under federal law (HIPAA), if the consent is not a HIPAA-compliant authorization, disclosures for health care operations are limited to the minimum necessary information to accomplish the intended purpose of the disclosure. Also, disclosures of information to another Participant for health care operations of the Participant that receives the information are only permitted if each entity either has or had a relationship with the patient, and the information pertains to such relationship.
The Statewide Collaboration Process: Policies and Procedures

governed by a QE and these individuals may Break the Glass if the following conditions are met:

i. Treatment may be provided to the patient without informed consent because, in the Practitioner’s or Advanced Emergency Medical Technician’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.

ii. The Practitioner or Advanced Emergency Medical Technician determines, in his or her reasonable judgment, that information that may be held by or accessible via the SHIN-NY governed by a QE may be material to emergency treatment.

iii. No denial of consent to access the patient’s information is currently in effect with respect to the Participant with which the Practitioner, Authorized User acting under the direction of a Practitioner or Advanced Emergency Medical Technician is affiliated.

iv. In the event that an Authorized User acting under the direction of a Practitioner Breaks the Glass, such Authorized User must record the name of the Practitioner providing such direction.

v. The Practitioner, Advanced Emergency Medical Technician or Authorized User acting under the direction of a Practitioner attests that all of the foregoing conditions have been satisfied, and the QE software maintains a record of this access.

b. Break the Glass access by an Authorized User acting under the direction of a Practitioner must be granted by a Practitioner on a case by case basis.

c. QEs shall ensure, or shall require their Participants to ensure, that access to information via the SHIN-NY governed by a QE without Affirmative Consent when treating a patient pursuant to this Section 1.2.3 terminates upon the completion of the emergency treatment.

d. Notwithstanding anything to the contrary set forth in these policies, a QE and its Participants shall not be required to exclude any Sensitive Health Information from access via the SHIN-NY governed by a QE where the circumstances set forth in this Section 1.2.3 are met.

e. QEs shall promptly notify their Data Suppliers that are federally-assisted alcohol or drug abuse programs when Protected Health Information from the Data Supplier’s records is accessed through the QE under this Section 1.2.3. This notice shall include (i) the name of the Participant that accessed the Protected Health Information; (ii) the name of the Authorized User within the Participant that accessed the Protected Health Information; (iii) the date and time of the access; and (iv) the nature of the emergency.
The Statewide Collaboration Process:  
Policies and Procedures

f. Upon a patient’s discharge from a Participant’s emergency room, if a Break the Glass incident occurred during the emergency room visit, the Participant shall notify the patient of such incident and inform the patient how he or she may request an audit log in accordance with Section 6.1.1(h) of these P&Ps. In lieu of providing such notice, Participants that are hospitals may notify all patients discharged from an emergency room that their PHI may have been accessed during a Break the Glass incident and inform patients how they may request an audit log to determine if such access occurred. The notice required by this Section shall be provided within ten days of the patient’s discharge and may be provided by the QE on behalf of the Participant.

1.2.4 Converting Data. Affirmative Consent shall not be required for the conversion of paper patient medical records into electronic form or for the uploading of Protected Health Information from the records of a Data Supplier to a QE, provided that (i) the QE is serving as the Data Supplier’s Business Associate (as defined in 45 C.F.R. § 160.103) and (ii) the QE does not make the information accessible to Participants until Affirmative Consent is obtained, except as otherwise permitted in these Policies and Procedures.

1.2.5 Improvement and Evaluation of QE Operations. Affirmative Consent shall not be required for a QE, government agencies or their contractors to access Protected Health Information via the SHIN-NY governed by a QE for the purpose of evaluating and improving QE operations. Consistent with HIPAA, access to PHI should be limited to the minimum amount necessary to accomplish the intended purpose of the use or disclosure.

1.2.6 De-Identified Data. Affirmative Consent shall not be required for access to De-identified Data for specified uses as set forth in Section 1.6.

1.2.7 Organ Procurement Organization Access. A QE may provide an Organ Procurement Organization with access to Protected Health Information without Affirmative Consent solely for the purposes of facilitating organ, eye or tissue donation and transplantation. A patient’s denial of Affirmative Consent for all Participants in a QE to access the patient’s Protected Health Information under Section 1.7.6 shall not prevent or otherwise restrict an Organ Procurement Organization from accessing the patient’s Protected Health Information through a QE for the purposes set forth in this Section 1.2.7

1.3 Form of Patient Consent. Except as otherwise permitted by the Patient Consent Transition Rules set forth at Section 1.8, consents shall be obtained through an Approved Consent. A QE may request approval to use a consent other than a Level 1 Consent or Level 2 Consent if it obtains approval from NYS DOH. Such approval will not be granted unless the alternative consent is substantially similar to the Level 1 Consent or Level 2 Consent, as applicable, and achieves the same basic purposes as such consents, as set forth in these Policies and Procedures.

1.3.1 Level 1 Uses. Affirmative Consent to access information via the SHIN-NY governed by a QE for Level 1 Uses shall be obtained using a Level 1 Consent or an alternative approved by NYS DOH under Section 1.3, which shall include the following information:

a. The information to which the patient is granting the Participant access, including specific reference to HIV, mental health, alcohol and substance abuse, reproductive health, sexually-transmitted disease, and genetic testing information;
The Statewide Collaboration Process: Policies and Procedures

b. The intended uses to which the information will be put by the Participant;

c. The relationship between the Participant and the patient whose information will be accessed;

d. A list of or reference to all Data Suppliers at the time of the patient’s consent, as well as an acknowledgement that Data Suppliers may change over time and instructions for patients to access an up-to-date list of Data Suppliers through a QE website or other means; the consent form shall also identify whether the QE is party to data sharing agreements with other QEs and, if so, provide instructions for patients to access an up-to-date list of Data Suppliers from a QE website or by other means;

e. Certification that only those engaged in Level 1 Uses may access the patient’s information;

f. Acknowledgement of the patient’s right to revoke consent and assurance that treatment will not be affected as a result;

1.3.2 Level 2 Uses. Consent to access information via the SHIN-NY governed by a QE for the purposes of Level 2 Uses shall be obtained using a Level 2 Consent or an alternative consent approved by NYS DOH under Section 1.3, which shall include (i) the information required of a Level 1 Consent pursuant to Section 1.3.1 and (ii) the following:

a. The specific purpose for which information is being accessed;

b. Whether the QE and/or its Participants will benefit financially as a result of the use/disclosure of the information to which the patient granting access;

c. The date or event upon which the patient’s consent expires;

d. Acknowledgement that payers may not condition health plan enrollment and receipt of benefits on a patient’s decision to grant or withhold consent.

1.3.3 Requirement for Separate Consents.

a. Consent for Level 1 Uses and consent for Level 2 Uses shall not be combined.

b. Consent for different Level 2 Uses shall not be combined.

c. A Consent for a Level 1 or Level 2 Use shall not be combined with any other document except with the approval of NYS DOH.
The Statewide Collaboration Process: Policies and Procedures

1.3.4 Education Requirement for Level 2 Consents Relating to Marketing. When a QE or its Participant obtains a Level 2 Consent to access Protected Health Information via the SHIN-NY governed by a QE for the purpose of Marketing, the QE or its Participant must provide the patient with information about the nature of such Marketing.

1.4 Sensitive Health Information.

1.4.1 General. An Affirmative Consent may authorize the Participant(s) listed in the consent to access all Protected Health Information referenced in the consent, including Sensitive Health Information.

1.4.2 Withholding Sensitive Health Information. QEs and Participants may, but shall not be required to, subject Sensitive Health Information to certain additional requirements, including but not limited to providing patients the option to withhold certain pieces of Sensitive Health Information from access via the SHIN-NY governed by a QE. In the event that a QE or a Participant has provided a patient the option to withhold certain pieces of Sensitive Health Information from access via the SHIN-NY governed by a QE, and the patient has exercised that option, the patient’s record when accessed via the SHIN-NY governed by a QE may, but is not required to, carry an alert indicating that data has been withheld from the record.

1.4.3 Redisclosure Warning

a. QEs shall include a warning statement that is viewed by Authorized Users whenever they are obtaining access to records of federally-assisted alcohol or drug abuse programs regulated under 42 C.F.R. Part 2 that contains the language required by 42 C.F.R. § 2.32. A QE may satisfy this requirement by placing such a redisclosure warning on all records that are made accessible through the QE.

b. QEs shall include a warning statement that is viewed by Authorized Users whenever they are obtaining access to HIV/AIDS information protected under Article 27-F of the N.Y. Public Health Law that contains the language required by Article 27-F. A QE may satisfy this requirement by (i) placing such a redisclosure warning on the same screen on which it places the redisclosure warning required at Section 1.4.3(a) or (ii) placing such a redisclosure warning on a log-in screen that Authorized Users must view before logging into their EHR or otherwise accessing the QE.

c. QEs shall include a warning statement that is viewed by Authorized Users whenever they are obtaining access to records of facilities licensed or operated by the New York State Office of Mental Health or the New York State Office for People With Developmental Disabilities that contains language notifying the Authorized User that such records may not be redisclosed except as permitted by the New York Mental Hygiene Law. A QE may satisfy this requirement by (i) placing such a redisclosure warning on the same screen on which it places the redisclosure warning required at Section 1.4.3(a) or (ii) placing such a redisclosure warning on a log-in screen that Authorized Users must view before logging into their EHR or otherwise accessing the QE.

1.4.4 Re-disclosure of Sensitive Health Information by Participants. Prior to re-disclosing Sensitive Health Information, Participants shall implement systems to identify and denote
The Statewide Collaboration Process: Policies and Procedures

Sensitive Health Information in order to ensure compliance with applicable state and federal laws and regulations governing re-disclosure of such information, including those applicable to HIV/AIDS, alcohol and substance abuse information, and records of facilities licensed or operated by the New York State Office of Mental Health or the New York State Office for People With Developmental Disabilities

1.5 Special Provisions Relating to Minors.

1.5.1 Exchange of Information for Minors under Ten Years of Age. QEs and their Participants may permit the exchange of information about minors below ten years of age based on an Affirmative Consent executed by the minor's parent or legal guardian.

1.5.2 Exchange of Minor Consent Information for Minors Ten Years of Age or Older.

a. QEs and their Participants shall permit the exchange of Minor Consent Information about minors ten years of age or older only when the minor has given consent to such exchange.

b. QEs shall require Participants to obtain a minor's consent to exchange Minor Consent Information at the time the services to which the minor is granting consent are provided.

c. QEs shall permit Participants providing health care services based on a minor's informed consent to access any Protected Health Information about the minor maintained by other Participants that is not Minor Consent Information based on the Affirmative Consent of the minor.

d. Notwithstanding the foregoing, a QE may permit the exchange of Protected Health Information about a minor without the minor's consent in accordance with Section 1.2.3 when treating a minor with an emergency condition.

1.5.3 Requirement to Obtain Minor's Consent When He or She Reaches the Age of Majority. QEs and their Participants shall not permit the exchange of Protected Health Information about patients age 18 years or older based on an Affirmative Consent of the patient's parent or legal guardian provided while the patient was a minor unless the parent or legal guardian continues to be the patient’s Personal Representative.

1.6 De-Identified Data.

1.6.1 Access of De-Identified Data for Specified Uses. Affirmative Consent shall not be required for a QE, a Participant, or a government agency to access De-Identified Data via the SHIN-NY governed by a QE for the following purposes:

a. Research approved by an Institutional Review Board organized and operating in accordance with 45 C.F.R. § 164; or

b. Any purpose for which the QE, Participant, or government agency may lawfully access Protected Health Information under the Policies and Procedures.
The Statewide Collaboration Process:  
Policies and Procedures

1.6.2 Creation of De-Identified Data for Specified Uses.  QEs may access Protected Health Information to create and validate the accuracy of De-Identified Data that is used in accordance with Section 1.6.1.

1.6.3 Other Requirements.

a. All other uses of De-Identified Data shall require Affirmative Consent.

b. A QE shall not condition a patient’s participation in the QE on the patient’s decision to consent or deny access to De-Identified Data for purposes other than those set forth in Section 1.6.1.

c. QEs shall, or shall require Participants to, comply with standards for the de-identification of data set forth in 45 C.F.R. § 164.514.

d. QEs shall, or shall require Participants or government agencies to, subject any use of De-Identified Data to adequate restrictions on the re-identification of such data.

1.7 Other Policies and Procedures Related to Consent.

1.7.1 Affiliated Practitioners. 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.

1.7.2 Authorized Users. An Affirmative Consent obtained by a Participant shall permit Authorized Users of the Participant to access information covered by the Affirmative Consent in accordance with Sections 2 and 4.

1.7.3 Consents Covering Multiple Participants. An Affirmative Consent may apply to more than one Participant provided that the consent (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 SHIN-NY governed by a QE pursuant to such consent and (ii) provides the patient with the option to select which of the Participants listed on the consent may access the patient's information via the SHIN-NY governed by a QE. Any Participant accessing information based on a consent covering multiple Participants must be identified on such consent at the time the patient grants Affirmative Consent.

1.7.4 Consent Obtained by QEs. QEs with the capacity to do so (through the provision of a personal health record or otherwise) may obtain consents on behalf of their Participants, provided such consents meet all of the requirements set forth in this Section 1.

1.7.5 Electronic Signatures. 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.
The Statewide Collaboration Process: 
Policies and Procedures

1.7.6 **Denial of Consent.** Consents shall give the patient the option of granting or affirmatively denying consent for individual Participants to access information about the patient via the SHIN-NY governed by a QE. A patient’s decision not to sign a consent shall not be construed as a “denial of consent” under Section 1.2.3(a)(iii). Each QE shall ensure that patients have the option, through the use of a single paper or electronic form, to affirmatively deny consent for all Participants in the QE to access the patient’s information, except as set forth in Section 1.2.2(b) or Section 1.2.7.

1.7.7 **Durability.** An Affirmative Consent for Level 1 Uses does not have to be time-limited. An Affirmative Consent for Level 2 Uses shall be time-limited and shall expire no more than two years after the date such Level 2 Consent is executed, except to the extent a longer duration is required to complete a Research protocol.

1.7.8 **Revocability.** Patients shall be entitled to revoke an Affirmative Consent at any time provided that such revocation shall not preclude any Participant that has accessed Protected Health Information via the SHIN-NY governed by a QE prior to such revocation and incorporated such Protected Health Information into its records from retaining such information in its records.

1.7.9 **Notification of a QE’s Data Suppliers.** QEs shall provide, or shall require their Participants to provide, patients with a list of or reference to all Data Suppliers at the time the QE or Participant obtains the patient’s Affirmative Consent. Each QE shall provide convenient access at all times thereafter, either through its website or otherwise, to a complete and accurate updated list of Data Suppliers.

1.7.10 **Compliance with Business Associate Agreements with Data Suppliers.** A QE shall execute a Business Associate Agreement with each Data Supplier. A QE shall not use or disclose Protected Health Information in any manner that violates the QE’s Business Associate Agreements.

1.7.11 **Disclosure to Vendors.** A QE, acting under the authority of a Business Associate Agreement with its Participants, may disclose Protected Health Information to vendors that assist in carrying out the QE’s authorized activities provided (i) the QE requires the vendors to protect the confidentiality of the Protected Health Information in accordance with the QE’s Business Associate Agreements with its Participants and (ii) the vendor does not make such information available to a Participant that has not obtained Affirmative Consent.

1.7.12 **Compliance with Existing Law.** All access to Protected Health Information via the SHIN-NY governed by a QE shall be consistent with applicable federal, state and local laws and regulations. If applicable law requires that certain documentation exist or that other conditions be met prior to accessing Protected Health Information 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.

1.7.13 **Compliance with Requests for Restrictions on Disclosures to a Payer Organization.** QEs shall develop processes to ensure that a Payer Organization does not access Protected Health Information through the QE if a patient has requested, in accordance with the HIPAA Privacy Rule and HITECH, that the Provider Organization creating such information not disclose it to the Payer Organization. While a QE may utilize any process...
The Statewide Collaboration Process: Policies and Procedures

that satisfies this requirement, a QE shall be deemed to have complied with the requirement if:

a. Upon a Provider Organization’s receipt of a patient’s request that Protected Health Information created by the Provider Organization not be disclosed to a Payer Organization, 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; and

b. Upon receipt of an Affirmative Consent covering a Payer Organization, the Payer Organization or QE notifies the patient in writing that his or her provision of the Affirmative Consent will revoke any prior request for a restriction on the disclosure of Protected Health Information by any Provider Organization to the Payer Organization, and the Affirmative Consent is rejected if the patient indicates he or she does not agree to the revocation of his or her prior request.

1.7.14 Development of Policies Governing Disclosures to Government Agencies for Health Oversight. QEs shall adopt policies governing the QE’s response to requests from government agencies for access to Protected Health Information for health oversight purposes, such as Medicaid audits, professional licensing reviews, and fraud and abuse investigations. Such policies shall address whether the QE will disclose information without Affirmative Consent in instances where disclosure is permitted but not required by law, and whether the QE will notify its Participants of such requests. This section does not cover access to Protected Health Information by Public Health Agencies under Section 1.2.2.

1.7.15 Indication of Presence of Medical Order for Life Sustaining Treatment (“MOLST”) or Other Advance Directive. QEs may note whether a patient has signed a MOLST or other advance directive in a Record Locator Service or Other Comparable Directory without Affirmative Consent.

1.7.16 Consent for Access by ACOs and IPAs. An Affirmative Consent authorizing access by an ACO or IPA shall cover only the ACO or IPA entity itself and not the health care providers participating in the ACO or IPA.

1.8 Patient Consent Transition Rules.

1.8.1 Use of Approved Consents. Except as set forth in Section 1.8.2, each QE shall be required to utilize an Approved Consent with respect to all patients who consent to the exchange of Protected Health Information via the SHIN-NY governed by a QE on or after the Consent Implementation Date.

1.8.2 Reliance on Existing Consents Executed Prior to the Consent Implementation Date. Each QE that obtained patient consent utilizing a patient consent substantially similar to a Level 1 Consent prior to the Consent Implementation Date (an “Existing Consent Form”) may continue to rely on such patient consent so long as such Existing Consent (i) complies with all applicable state and federal laws and regulations and (ii) if such Existing Consent is relied upon for the release of HIV-related information, such Existing Consent has been approved by NYS DOH.
1.8.3 Use of Existing Consent After Consent Implementation Date. A QE may continue to use an Existing Consent after the Consent Implementation Date if the Existing Consent is approved by NYS DOH under Section 1.3.

1.9 Receipt of Patient Care Alerts.

1.9.1 A Participant may receive Patient Care Alerts from a QE with respect to any patient from whom the Participant has obtained Affirmative Consent.

1.9.2 Patient Care Alerts containing Protected Health Information shall be sent 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.
The Statewide Collaboration Process:
Policies and Procedures

SECTION 2: AUTHORIZATION

Purpose/Principles

Authorization is the process of determining whether a particular individual within a Participant has the right to access Protected Health Information via the SHIN-NY governed by a QE. Authorization is based on role-based access standards that take into account an individual’s job function and the information needed to successfully carry out a role within the Participant. This Section 2 sets forth minimum requirements that QEs and their Participants shall follow when establishing role-based access standards and authorizing individuals to access information about a patient via the SHIN-NY governed by a QE. They are designed to limit exchange of information to the minimum necessary for accomplishing the intended purpose of the exchange, thereby allowing patients to have confidence in the privacy of their health information as it moves among Participants in a QE.

Policies and Procedures

2.1 Role-Based Access Standards.

2.1.1 QEs shall establish and implement policies and procedures that:

a. Establish categories of Authorized Users;

b. Define the purposes for which Authorized Users in those categories may access Protected Health Information via the SHIN-NY governed by a QE; and

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

2.1.2 The purposes for which an Authorized User may access information via the SHIN-NY governed by a QE and the types of information an Authorized User may access shall be based, at a minimum, on the Authorized User’s job function and relationship to the patient.

2.1.3 At a minimum, QEs shall utilize the following role-based access standards to establish appropriate categories of Authorized Users and to define the purposes for which access may be granted and the types of information that may be accessed:

a. Break the Glass - a (i) Practitioner; (ii) Authorized User acting under the direction of a Practitioner; or (iii) Advanced Emergency Medical Technician who, under the provisions of §1.2.3 (‘Break the Glass’) has temporary rights to access Protected Health Information for a specific 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 administrators with access to non-clinical information;
The Statewide Collaboration Process: Policies and Procedures

f. QE administrators with access to clinical information in order to engage in public health reporting in accordance with Section 1.2.2 of these Policies and Procedures or other activities authorized under these Policies and Procedures; and

g. QE or Participant administrators with access to clinical and non-clinical information for purposes of system maintenance and testing, troubleshooting and similar operational and technical support purposes.

2.1.4 QEs shall require Participants to designate the individuals within their organizations who will be authorized to access information via the SHIN-NY governed by a QE and to assign those individuals to the appropriate categories as listed above.

2.1.5 QEs and Participants shall identify individuals (including individuals encompassed within the role-based access category defined at §2.1.3(g)) whose access to data may bypass or enable circumvention of activity logging, access controls, or other security controls. These Authorized Users shall be subject to heightened scrutiny both in hiring and in ongoing auditing and monitoring of their activities. Such heightened scrutiny may include pre-employment (or pre-engagement for contractors) background checks; mandatory privacy and security training and annual retraining; a formal termination procedure more stringent and timely than that set forth in §4.8; regular review of access privileges, user accounts; or other measures as the QE or Participant may deem appropriate given their security risk assessment.

2.1.6 QEs may permit Certified Applications to access Protected Health Information via the SHIN-NY in accordance with the terms of these Policies and Procedures. Each QE’s certification process for Certified Applications must satisfy all encryption and other security standards incorporated into the SHIN-NY Policy Standards through the SCP.
The Statewide Collaboration Process:  
Policies and Procedures

SECTION 3: AUTHENTICATION

Purpose/Principles

Authentication is the process of verifying that an individual who has been authorized and is seeking to access information via the SHIN-NY governed by a QE is who he or she claims to be. This is accomplished by providing proof of identity. This Section 3 sets forth minimum requirements that QEs and their Participants shall follow when authenticating individuals prior to allowing them to access information via the SHIN-NY governed by a QE. These Policies and Procedures represent an important technical security safeguard for protecting a patient’s information from various internal and external risks, including unauthorized access.

Policies and Procedures

3.1 Obligation to Ensure Authentication of Identity of Authorized User Prior to Access. QEs shall authenticate, or shall require their Participants to authenticate, each Authorized User's identity prior to providing such Authorized User with access to Protected Health Information via the SHIN-NY governed by a QE. Such authentication shall take place in accordance with the provisions of this Section 3.

3.2 Authentication Requirements.

3.2.1 Authentication Standard. Until such time as a determination is made, pursuant to Section 3.2.2, to utilize a higher authentication standard, QEs shall authenticate, or shall require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Identity Level of Assurance 2 (“Level 2”) set forth in National Institute of Standards and Technology Special Publication 800-63 (hereinafter, “NIST SP 800-63”).

a. Level 2 will require, among other technical specifications, QEs or their Participants to authenticate each Authorized User's identity using only single-factor authentication, which queries Authorized Users for something they know (e.g., a password). Under Level 2, QEs or their Participants will be free to use only a password, and need not use it in combination with any other tokens, provided it protects against online guessing and replay attacks. Level 2 will require QEs or their Participants to implement initial identity-proofing procedures (either remote or in-person) that require Authorized Users to provide identifying materials and information upon application for access to information through the QE.

3.2.2 Transitional Authentication Standard. In light of the importance of strong security measures to the protection of patient data and the transition of certain organizations and entities, including but not limited to the New York State Medicaid Program, toward utilization of an authentication methodology that meets the minimum technical requirements for Identity Level of Assurance 3 (“Level 3”) set forth in NIST SP 800-63, NYeC shall, through the SCP, establish a Work Group to consider the cost, workflow, and other issues implicated by a transition to Level 3, and determine the implementation approach and timetable for transition to Level 3. Upon notice from NYeC that an implementation approach and timetable has been agreed upon, QEs shall be required to authenticate, or require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum requirements for Level 3.
The Statewide Collaboration Process:
Policies and Procedures

a. Level 3 will require, among other technical specifications, QEs or their Participants to authenticate each Authorized User’s identity using multifactor authentication, which queries Authorized Users for something they know (e.g., a password) and something they have (e.g., an ID badge or a cryptographic key). QEs or their Participants will be free to use a combination of tokens (authentication secrets to which an Authorized User’s identity is bound), including soft cryptographic tokens with the key stored on a general-purpose computer, hard cryptographic tokens, which have the key stored on a special hardware device like a key FOB, or one-time password device tokens, which have a symmetric key stored on a personal hardware device (e.g., a cell phone) in a manner that protects against protocol threats, including eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks. In addition to use of multifactor authentication, Level 3 will require QEs or their Participants to implement initial identity-proofing procedures (either remote or in person) that require Authorized Users to provide identifying materials and information (e.g., a valid current primary Government Picture ID and either address of record or nationality, such as a driver’s license or passport) upon application for access to information through the QE, though these requirements will be more stringent than those set forth at Level 2.

3.2.3 Choice of Technical Solution. In meeting the requirements set forth in this Section 3.2, QEs and their Participants may select the best available authentication methodology, consistent with guidance set forth in NIST SP 800-63, based on individual assessments of their technical architectures, network sizes, and policies.

3.3 Compliance with Policies Resulting from Statewide Risk Analysis. In the event that New York State conducts a statewide risk analysis of the potential harm and likelihood of adverse impacts that could result from an error in identity authentication within the SHIN-NY that indicates that authentication policies and procedures that differ from, or are in addition to, those set forth in this Section 3, should be adopted, any such authentication policies and procedures shall be developed and approved through the SCP before adoption.

3.4 Option to Rely on Statewide Authentication Service. In the event that New York State develops statewide services for the authentication of Authorized Users, QEs may utilize such statewide services to authenticate an Authorized User in accordance with the provisions of this Section 3.

3.5 Authentication of Certified Applications and Downstream Users. QEs permitting access to the SHIN-NY by Participants through Certified Applications must (i) implement systems consistent with the SHIN-NY Policy Standards for authenticating a Certified Application’s credentials in connection with each access request; and (ii) require each Participant accessing Protected Health Information through a Certified Application to authenticate the Participant’s users in a manner consistent with Section 3 of these Policies and Procedures.
The Statewide Collaboration Process:  
Policies and Procedures

SECTION 4: ACCESS

Purpose/Principles

Access controls govern when and how a patient’s information may be accessed by Authorized Users through a QE’s Participant. This Section 4 sets forth minimum behavioral controls QEs shall implement to ensure that: 1.) only Authorized Users and Certified Applications access information via the SHIN-NY governed by a QE; and 2.) they do so only in accordance with patient consent and with other requirements (specified herein) that limit their access to specified information (e.g., that which is relevant to a patient’s treatment). These access policies, coupled with informed patient consent, are designed to reduce unauthorized access and ensure information is used for authorized purposes.

Policies and Procedures

4.1 General. QEs shall, or shall require their Participants to, ensure that each Authorized User is assigned a unique user name and password to provide such Authorized User with access to patient information via the SHIN-NY governed by a QE. In doing so, QEs and/or their Participants shall comply with the following minimum standards:

4.1.1 Authorized Users shall be authenticated in accordance with the provisions of Section 3.

4.1.2 Passwords shall meet the password strength requirements set forth in NIST SP 800-63 (e.g. the probability of success of an online password guessing attack shall not exceed 1 in 16,384 over the life of the password).

4.1.3 Group or temporary user names shall be prohibited.

4.1.4 Authorized Users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing passwords.

4.1.5 Authorized Users shall be prohibited from sharing their user names and/or passwords with others and from using the user names and/or passwords of others.

4.2 Authorized Purposes. QEs and their Participants shall permit Authorized Users to access Protected Health Information of a patient via the SHIN-NY governed by a QE only for purposes consistent with a patient’s Affirmative Consent or an exception set forth in Section 1.2

4.3 Failed Access Attempts. QEs shall enforce a limit of consecutive Failed Access Attempts by an Authorized User. Upon a fifth Failed Access Attempt, QEs shall ensure that said Authorized User’s access to the QE is disabled either by locking the account until release by a QE administrator or by locking the account for a specific period of time as specified by the QE, after which the Authorized User may reestablish access using appropriate identification and authentication procedures. If Authorized Users access the SHIN-NY governed by a QE by logging on to a Participant’s information system (without the need for a separate QE log-on), the QE may delegate to the Participant responsibility for enforcing this Failed Access Attempt limitation.

4.4 Periods of Inactivity. QEs shall ensure that an Authorized User is automatically logged out of the QE after a period of inactivity by such Authorized User. The termination shall remain in effect until the Authorized User reestablishes access using appropriate identification and authentication procedures. QEs shall establish the length of periods of inactivity that will trigger such termination
based on their internal risk analyses as well organizational factors such as current technical infrastructure, hardware and software security capabilities.

4.5 **Access Limited to Minimum Necessary Information.** QEs shall, and shall require their Participants to, ensure that reasonable efforts are made, except in the case of access for Treatment, to limit the information accessed via the SHIN-NY governed by a QE to the minimum amount necessary to accomplish the intended purpose for which the information is accessed.

4.6 **Record Locator Service and Other Comparable Directories.** In operating a Record Locator Service or Other Comparable Directory, QEs shall, or shall require their Participants to:

4.6.1 Implement reasonable safeguards to minimize unauthorized incidental disclosures of Protected Health Information during the process of identifying a patient and locating a patient's medical records.

4.6.2 Include the minimum amount of demographic information reasonably necessary to enable Authorized Users to successfully identify a patient through the Record Locator System.

4.6.3 Prohibit Authorized Users from accessing Protected Health Information in any manner inconsistent with these Policies and Procedures.

4.7 **Training.** The behavioral and organizational access controls set forth above will only be effective if 1) a QE’s health information access policies and procedures are clear; and 2) Authorized Users understand the policies and procedures and their responsibilities within such policies and procedures. As such, QEs shall implement, either directly or through Participants, minimum training requirements for educating individuals about the policies and procedures for accessing Protected Health Information via the SHIN-NY governed by a QE as specified by the Statewide Collaboration Process

4.7.1 QEs shall, or shall require their Participants to, provide either on-site training, web-based training, or comparable training tools so that Authorized Users are familiar with the operation of the QE and the policies and procedures governing access to information via the SHIN-NY governed by a QE.

4.7.2 QEs shall, or shall require their Participants to, ensure that each Authorized User undergoes such training prior to being granted access to information via the SHIN-NY governed by a QE.

4.7.3 QEs shall, or shall require their Participants to, ensure that each Authorized User signs a certification that he or she has received training and will comply with the QE’s policies and procedures. Such certification may be made on a paper form or electronically and shall be retained by QEs or their Participants for at least six years.

4.7.4 QEs shall ensure that each Authorized User undergoes continuing and/or refresher training on an annual basis as a condition of maintaining authorization to access patient information via the SHIN-NY governed by a QE. QEs shall ensure that records of such training are maintained and available for audit for a period of at least six years.
The Statewide Collaboration Process: Policies and Procedures

4.8 Termination of Access and Other Sanctions. QEs shall develop policies and procedures to terminate, or to require their Participants to terminate, the access of Authorized Users and/or to impose sanctions as necessary.

4.8.1 QEs shall ensure that access to the QE of a Participant (and all of the Participant’s Authorized Users, if applicable) is terminated in the following situations and in accordance with the processes described:

a. Immediately or as promptly as reasonably practicable but in any event within one business day of termination of a Participant’s Participation Agreement with the QE; and/or

b. Immediately or as promptly as reasonably practicable but in any event within one business day of notification of termination of an Authorized User’s employment or affiliation with the Participant.

4.8.2 In order to comply with Section 4.8.1(b), QEs shall require their Participants to notify the QE upon termination of an Authorized User’s employment or affiliation with the Participant immediately or as promptly as reasonably practicable but in any event within one business day of termination.

4.8.3 QEs shall establish sanctions to redress policy or procedural violations. Sanctions could include temporary access prohibitions, re-training requirements, termination, or other processes the QE deems necessary in accordance with its internal risk analyses.

4.8.4 The SCP shall consider developing guidance on the following to be included in future versions of these Policies and Procedures: Whether state level sanctions should be developed and implemented by QEs.

4.9 Access by Certified Applications.

4.9.1 Notwithstanding anything to the contrary in this Section 4, a QE may allow a Certified Application to access Protected Health Information through the SHIN-NY in accordance with the terms of these Policies and Procedures.

4.9.2 As a condition of granting such access, a QE shall require a Participant using a Certified Application to provide the QE with (i) the name and contact information of the individual responsible for requesting access through the Certified Application on the Participant’s behalf and (ii) a certification signed by such individual acknowledging that he or she is personally responsible for the use of the Certified Application for this purpose. The Participant shall be required by the QE to update this information and provide a new certification prior to changing the individual responsible for the use of the Certified Application.

4.9.3 The QE shall require a Participant using a Certified Application to limit access to any Protected Health Information obtained through the Certified Application to individual users of the Participant’s information system who would be eligible to be Authorized Users of the Participant under these Policies and Procedures if they were accessing Protected Health Information directly through the QE. The QE shall also require the Participant to credential, train and otherwise manage the access of such users to Protected Health Information.
The Statewide Collaboration Process: Policies and Procedures

obtained through the QE in accordance with the provisions of this Section 4 applicable to Authorized Users.

4.10 Participation Agreements

4.10.1 Except as set forth otherwise in Section 4.10.2, a QE shall enter into a Participation Agreement directly with each of its Participants. Participation Agreements shall require Participants to comply with these Policies and Procedures, as they may be amended from time to time.

4.10.2 A QE may enter into a Participation Agreement with a Provider Organization that covers Practitioners participating in an electronic health information exchange maintained by the Provider Organization if:

a. The Provider Organization enters into a written agreement with each Practitioner or medical group comprised of Practitioners in a form acceptable to the QE that obligates the Practitioner(s) to abide by the relevant terms of the Provider Organization’s Participation Agreement with the QE and engage in bi-directional exchange of Protected Health Information through the SHIN-NY.

b. The Provider Organization, under its Participation Agreement with the QE, assumes responsibility for the training and oversight of the Practitioners under these Policies and Procedures as if the Practitioners were Authorized Users of the Provider Organization.

c. The Provider Organization, under its Participation Agreement with the QE, accepts liability for the acts and omissions of such Practitioners for violations of the Provider Organization’s Participation Agreement with the QE as if such Practitioners were Authorized Users of the Provider Organization.

4.10.3 Notwithstanding a Provider Organization’s responsibilities with respect to Practitioners participating in a QE through the Provider Organization under Section 4.10.2, each Practitioner or medical group entering into a written agreement with the Provider Organization shall be treated as a separate Participant for purposes of implementing the patient consent requirements of these Policies and Procedures.

4.10.4 Sections 4.10.2 and 4.10.3 shall not apply to Practitioners when they are acting as Affiliated Practitioners of a Provider Organization under Section 1.7.1.
The Statewide Collaboration Process:
Policies and Procedures

SECTION 5: PATIENT ENGAGEMENT AND ACCESS

Purpose/Principles

QEs present an opportunity for patients to gain access to their health information through a single electronic portal, thereby eliminating many of the bureaucratic hurdles patients currently endure when attempting to obtain copies of their medical records. Openness about policies, procedures, technology, and practices among Participants exchanging health information via the SHIN-NY governed by a QE is a foundational principle essential to protecting patient privacy and to realizing the potential for QEs to markedly improve patient access to their own health information. This Section 5 sets forth minimum requirement QEs and their Participants shall follow to ensure that patients are able to understand what information exists about them, how that information is used, and how they can access such information.

Policies and Procedures

5.1 QEs shall be required to educate patients and/or their Personal Representatives with respect to the consent process and the terms and conditions upon which their Protected Health Information can be shared with Authorized Users, including conforming to any patient education program standards developed through the SCP, and informing the patient and/or his or her Personal Representative of the benefits and risks of providing an Affirmative Consent for his or her Protected Health Information to be shared through the QE.

5.2 QEs shall, or shall require their Participants to, develop and educate patients and/or their Personal Representatives with respect to policies related to patients' rights to access their own Protected Health Information. At the current time, QEs are not required to provide patients and/or their Personal Representatives with access to their own Protected Health Information, but they are encouraged to do so and are required to inform patients as to whether such access is available to them. If such access is not available directly through the QE, the QE shall inform the patient and/or their Personal Representative that they may access their Protected Health Information by contacting their health care providers. If a QE chooses to provide patients with access to their Protected Health Information, the QE must provide such access to a patient’s Personal Representative upon request.

5.3 To facilitate informed consent and to ensure that patients know where information about them is being generated, QEs shall provide, or shall require their Participants to provide, patients with (i) notice – in a manner easily understood by patients – that their Protected Health Information is being uploaded to a QE; (ii) a list of or reference to all Data Suppliers (consistent with Section 1.7.9); (iii) information about how to contact Data Suppliers; and (iv) a description of how patients may deny consent for all QE Participants to access their Protected Health Information through the QE in accordance with Section 1.7.6. QEs and their Participants shall participate in any applicable patient education programs developed by the State Designated Entity through the SCP for the purpose of educating patients about the uploading of their Protected Health Information to a QE.

5.4 If patient access to Protected Health Information is provided by a QE, the QE shall inform the patient as to all material terms and conditions relating to such access. Access of patients or their Personal Representatives to Protected Health Information must be in accordance with all applicable laws and regulations, including but not limited to PHL §18, MHL § 33.16 and 10 NYCCR § 58-1.8. For example, access of patients or their Personal Representatives must be in accordance with federal and state laws permitting denial of access to medical information if, in the exercise of professional
The Statewide Collaboration Process: Policies and Procedures

judgment, a licensed health care professional believes that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.

5.5 Each QE shall develop a plan and process for assuring meaningful patient/consumer input and participation in QE operations and decision making. Each QE is strongly encouraged to include various consumer perspectives on its Board of Directors, and to use such methods as Patient/Consumer Advisory Committees to generate broad input and participation in the design and implementation of QE policies and procedures.

5.6 As required in Section 6.4, QEs shall, or shall require their Participants to, provide patients with information about how their Protected Health Information was accessed through the QE.

5.7 QEs shall direct patients to the appropriate Participants who can assist them in a timely fashion to resolve an inquiry or dispute over the accuracy or integrity of their Protected Health Information, and to have erroneous information corrected or to have a dispute documented if their request to revise data is denied.

5.8 Each QE shall require its Participants and Data Suppliers to notify the QE if, in response to a request by a patient, the Participant or Data Supplier makes any corrections to the patient’s erroneous information.

5.9 Each QE shall make reasonable efforts to provide its Participants with information indicating which other QE Participants have accessed erroneous information that the Participant has corrected at the request of patients in accordance with Section 5.7.
The Statewide Collaboration Process: Policies and Procedures

SECTION 6: AUDIT

Purpose/Principles

Audits are useful oversight tools for recording and examining access to information through a QE (e.g., who accessed what data and when) and are necessary for verifying compliance with access controls, like those specified in Section 4, developed to prevent/limit inappropriate access to information. This Section 6 sets forth minimum requirement that QEs and their Participants shall follow when logging and auditing access to health information via the SHIN-NY governed by a QE.

Policies and Procedures

6.1 Maintenance of Audit Logs. Each QE shall maintain Audit Logs that document all access of Protected Health Information via the SHIN-NY governed by a QE.

   6.1.1 Audit Logs shall, at a minimum, include the following information:

   a. The identity of the patient whose Protected Health Information was accessed;
   b. The identity of the Authorized User accessing the 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. The 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); and
   g. Unsuccessful access (log-in) attempts; and
   h. Whether access occurred through a Break the Glass incident.

6.1.2 With respect to access to Protected Health Information through a QE by a Certified Application, the Audit Log shall include each instance in which such Protected Health Information was accessed (i) by the Certified Application through the QE and (ii) by an individual user of the Participant through the Participant’s system.

6.1.3 With respect to access to Protected Health Information through a QE by an Authorized User of a Public Health Agency, QEs shall track at the time of access the reason(s) for each Authorized User’s access of Protected Health Information.

6.1.4 Audit Logs shall be immutable. An immutable Audit Log requires either that log information cannot be altered by anyone regardless of access privilege or that any alterations are tamper evident.
6.1.5 Audit Logs shall be maintained for a period of at least six years from the date on which information is accessed.

6.2 **Obligation to Conduct Periodic Audits.** Each QE shall conduct, or shall require each of its Participants to conduct, periodic audits to monitor use of the QE by Participants and their Authorized Users and ensure compliance with the Policies and Procedures and all applicable laws, rules and regulations.

6.2.1 At a minimum, the QE shall audit, or require its Participants to audit, the following:
   a. That Affirmative Consents are on file for patients whose Protected Health Information is accessed via the SHIN-NY governed by a QE, other than in Break the Glass situations;
   b. That Authorized Users who access Protected Health Information via the SHIN-NY governed by a QE do so for Authorized Purposes; and
   c. That applicable requirements were met where Protected Health Information was accessed through a Break the Glass incident.

6.2.2 If a Participant accesses Protected Health Information via the SHIN-NY through a Certified Application, the audits described in Section 6.2.1 shall include access by the Participant’s users through the Participant’s system.

6.2.3 The activities of all or a statistically significant subset of a QE’s Participants shall be audited.

6.2.4 Periodic audits shall be conducted at least on an annual basis. QEs shall consider their own risk analyses and organizational factors, such as current technical infrastructure, hardware and software security capabilities and whether access was obtained through a Certified Application, to determine the reasonable and appropriate frequency with which to conduct audits more often than annually. Notwithstanding the foregoing, all Break the Glass incidents shall be audited.

6.2.5 Periodic audits shall be conducted using a statistically significant sample size.

6.2.6 If audits are conducted by Participants rather than by the QE, the QE shall:
   a. Require each Participant to conduct the audit within such time period as reasonably requested by the QE; and
   b. Require each Participant to report the results of the audit to the QE within such time period and in such format as reasonably requested by the QE.

6.3 **Participant Access to Audit Logs.**

6.3.1 A QE shall provide the Participant, upon request, with the following information regarding any patient of the Participant whose Protected Health Information was accessed via the SHIN-NY governed by a QE:
The Statewide Collaboration Process: Policies and Procedures

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; and

c. The type of Protected Health Information or record that was accessed (e.g., clinical data, laboratory data, etc.).

6.3.2 A Participant shall only be entitled to receive audit log information pursuant to Section 6.3.1 for patients who have provided Affirmative Consent for that Participant to access his or her Protected Health Information.

6.3.3 QEs shall provide such information as promptly as reasonably practicable but in no event more than 10 calendar days after receipt of the request.

6.4 Patient Access to Audit Information.

6.4.1 Each QE shall, or shall require its Participants to, provide patients, upon request, with the following information:

a. The name and role (e.g., physician) 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 such Protected Health Information;

c. The time and date of such access; and

d. The type of Protected Health Information or record that was accessed (e.g., clinical data, laboratory data, etc.).

6.4.2 QEs shall, or shall require their Participants to provide such information as promptly as reasonably practicable but in no event more than ten calendar days after receipt of the request.

6.4.3 If requested, QEs shall, or shall require their Participants to, provide such information to patients at no cost once in every 12-month period. QEs may establish a reasonable fee for any additional requests within a given 12-month period; provided that the QE shall waive any such fee where such additional request is based on a patient’s allegation of unauthorized access to the patient’s Protected Health Information via the SHIN-NY governed by a QE.

6.4.4 If applicable, QEs shall, or shall require their Participants to, provide notice of the availability of such information on any patient portals maintained by the QE or its Participants.

6.5 Public Availability of Audits. Each QE shall make the results of its periodic audit available on the QE’s website. Such results shall be made available as promptly as reasonably practicable, but in any event not more than 30 days after completion of the audit.
6.6 **Correction of Erroneous Data.** In the most expedient time possible and without unreasonable delay, each QE shall investigate (or require the applicable Participant to investigate) the scope and magnitude of any data inconsistency or potential error that was made in the course of the QE’s data aggregation and exchange activities and, if an error is determined to exist, identify the root cause of the error and ensure its correction. QEs shall log all such errors, the actions taken to address them and the final resolution of the error. QEs shall also make reasonable efforts to identify Participants that accessed such erroneous information and to notify them of corrections. This provision does not apply to updates to data that are made by Data Suppliers in the ordinary course of their clinical activities nor does it apply to updates to Demographic Information.

6.7 **Weekly Audit Reports by Organ Procurement Organizations.** QEs shall require weekly confirmation by Organ Procurement Organizations that all instances in which Protected Health Information was accessed through the QE by the Organ Procurement Organization’s Authorized Users were consistent with the terms of these Policies and Procedures (based upon a listing sent by the QE).

6.8 **Additional Requirements Related to Auditing of Public Health Access.** QEs shall use special safeguards with respect to audits of access by Public Health Agencies, which shall include at least the following:

6.8.1 The QE shall create, on a regular basis, an audit report of Authorized User activity for each Public Health Agency workgroup that will include, at a minimum, the patient names, times, dates and reason for access for each Authorized User.

6.8.2 The name of the particular Public Health Agency shall be listed in the patient audit logs.

6.8.3 The QE shall follow-up with workgroup manager(s) if approval of an audit report is not received. If the attempt to contact the workgroup manager(s) is unsuccessful, the QE may suspend all Authorized User accounts associated with that particular workgroup until the situation is resolved.
Purpose/Principles

While the consent, authorization, authentication, access, and audit policies above are designed to protect patients from privacy breaches, they have little weight if QEs and their Participants are not held accountable and to certain behavioral standards when privacy violations occur. This Section 7 sets forth minimum standards QEs and their Participants shall follow in the event of a breach. They are designed to hold violators accountable for violations, assure patients about the QE’s commitment to privacy, and mitigate any harm that privacy violations may cause.

Policies and Procedures

7.1 Obligation of Participants to Report Actual or Suspected Breaches. Each QE shall require its Participants to notify the QE in the event that a Participant becomes aware of any actual or suspected Breach of Unsecured Protected Health Information accessed via the SHIN-NY governed by a QE.

7.1.1 Notification shall be made in the most expedient time possible and without unreasonable delay.

7.1.2 Notification shall be made in writing.

7.2 Responsibilities of the QE.

7.2.1 QEs shall be required to develop a Breach plan as part of their policies and procedures. The plan shall provide that, in the event the QE becomes aware of any suspected Breach of Unsecured Protected Health Information, either through notification by a Participant or otherwise, the QE must, in the most expedient time possible and without unreasonable delay, investigate (or require the applicable Participant to investigate) the scope and magnitude of such suspected Breach, determine whether an actual Breach has occurred and, if so, identify the root cause of the Breach.

7.2.2 In the event it is determined that an actual Breach has occurred, the QE must, at a minimum:

a. Notify any Participants whose Protected Health Information was subject to the Breach.

b. Mitigate (or require the applicable Participant to mitigate) to the extent practicable, any harmful effect of such Breach that is known to the QE or the Participant. QEs’ mitigation efforts shall correspond with and be dependent upon their internal risk analyses. Notify (or require the applicable Participant to notify) the patient and any applicable regulatory agencies as required by and in accordance with applicable federal, state and local laws and regulations, including but not limited to HITECH.
SECTION 8: HIPAA COMPLIANCE

Purpose/Principles

While it is anticipated that most Participants will be Covered Entities and thus subject to the HIPAA Privacy Rule and HIPAA Security Rule, there may be some Participants that are not Covered Entities. The provisions of this Section 8 are designed to ensure that entities accessing Protected Health Information through a QE abide by the same applicable HIPAA requirements as Covered Entities even if they are not otherwise legally obligated to do so.

Policies and Procedures

8.1 Each Participant that is a Covered Entity shall comply with the HIPAA Privacy Rule and HIPAA Security Rule.

8.2 Each Participant that is not a Covered Entity shall adopt all of the applicable administrative, physical and technical safeguards set forth in the HIPAA Security Rule as well as the restrictions on the use and disclosure of Protected Health Information set forth in the HIPAA Privacy Rule.
The Statewide Collaboration Process: 
Policies and Procedures

SECTION 9: SANCTIONS

Purpose/Principles

Sanctions are an important mechanism for ensuring that Participants and Authorized Users comply with these Policies & Procedures. The provisions in this Section 9 are designed to provide guidelines for the imposition of sanctions by QEs and their Participants while leaving flexibility for QEs and their Participants to determine appropriate sanctions on a case by case basis.

Policies and Procedures

9.1 Each QE shall establish policies consistent with this Section 9 governing the imposition of sanctions on Participants and their Authorized Users who violate the terms of these Policies and Procedures. QEs shall apply, or require their Participants to apply, sanctions under such policies in the event of such violations. QEs and/or their Participants and Public Health Agencies shall inform all Authorized Users about the QE’s sanctions policies.

9.2 When determining the type of sanction to apply, QEs and/or their Participants shall take into account the following factors: (i) whether the violation was a first time or repeat offense; (ii) the level of culpability of the Participant or Authorized User, e.g., whether the violation was made intentionally, recklessly or negligently; (iii) whether the violation constitutes a crime under state or federal law; and (iv) whether the violation resulted in harm to a patient or other person.

9.3 Sanctions shall include, but do not necessarily have to be limited to: (i) requiring an Authorized User to undergo additional training with respect to participation in the QE; (ii) temporarily restricting an Authorized User's access to the QE; (iii) terminating the access of an Authorized User to the QE; (iv) suspending or terminating a Participant's participation in the QE; and (v) the assessment of fines or other monetary penalties.
See approved Level 1 Single Provider Consent, Level 1 Multi-Provider Consent, and Level 1 Payer Consent available on the NYeC website at http://www.nyehealth.org/SCP-policies.
The Statewide Collaboration Process: Policies and Procedures

APPENDIX B: MODEL LEVEL 2 CONSENTs

See approved model Level 2 Payer Consent for Payment available on the NYeC website at http://www.nyehealth.org/SCP-policies.
INTRODUCTION

The purpose of this document is to provide a high level description of the procedures by which the Oversight Entity (as defined below) or its designee will perform basic oversight over Qualified Entities (QEs). This includes requirements for routine internal QE self-audits, procedures for complaint handling, external monitoring, audits, and investigations as well as any enforcement actions that may result from those activities by the Oversight Entity.

Out of scope for this document are activities related to (a) responding to allegations of privacy breaches, which are to be handled in accordance with applicable law and the SHIN-NY Policy Standards Privacy and Security Policies and Procedures for QEs and their Participants, (b) investigations in response to subpoenas from law enforcement and other government agencies and (c) responding to allegations of breach of the Qualified Entity Participation Agreement.

Alleged privacy breaches and investigations by government agencies are to be reported to the Oversight Entity and may result in the Oversight Entity initiating additional investigations and audits as it sees fit to perform adequate oversight. Those additional investigations and audits would follow the procedures described in the external audit and/or investigation section of the policies and procedures described herein.

In order for a QE to participate in the SHIN-NY, a QE must comply with applicable State, Federal and local law and the Certification Requirements, which are designed to protect and maintain the reliability, accuracy and integrity of the SHIN-NY. The Certification Requirements fall into the following four categories, and such categories are more specifically described in the Qualified Entity (QE) Organizational Characteristics Requirements, as amended from time-to-time:

- Organizational Characteristics
- Operational Requirements
- Policies and Procedures
- Technical Services

The Oversight and Enforcement Policies set forth mechanisms for ensuring that (a) QEs comply with applicable State, Federal and local law and the Certification Requirements and (b) appropriate action is taken to respond to and/or remedy non-compliance. Together with the Certification Process, implementation of the Oversight and Enforcement Policies will allow for oversight, monitoring and enforcement of applicable State, Federal and local law and the Certification Requirements.

DEFINITIONS

All capitalized terms used and not defined herein shall have the respective meanings given to such terms in the Privacy and Security Policies and Procedures for QEs and their Participants in New York State, as amended from time-to-time (the “Policies and Procedures”).

Appeals Committee means the committee designated by the Oversight Entity (NYS DOH) to review and adjudicate all appeals submitted by the QE in response to imposition of a Remedy related to non-compliance of applicable State, Federal and local law or one or more of the Certification Requirements.

Certification Process has the meaning set forth in the Qualified Entity (QE) Organizational Characteristics Requirements, as amended from time-to-time.

Non-Compliance means an occurrence that is inconsistent with or violates applicable State, Federal and local law or the Certification Requirements relating to a QE or its Participants.
NYS DOH means the New York State Department of Health.

Oversight Entity means the entity responsible for implementing and overseeing the Oversight and Enforcement Policies and for establishing remedies. Periodic monitoring of QEs shall be the responsibility of NYS DOH or a third-party designated by NYS DOH.

Certification Body is the third-party entity designated by NYS DOH to conduct periodic auditing and monitoring of QEs.

Certification Requirements has the meaning set forth in the Qualified Entity (QE) Organizational Characteristics Requirements, as amended from time-to-time.

Remedy means actions imposed on a QE in connection with Non-Compliance in accordance with the policies and procedures described herein.

Stakeholder includes but may not be limited to parties interested in providing or obtaining information from the SHIN-NY and includes consumers/patients, caregivers, physicians and clinicians, hospitals, payers including Medicaid and Medicare, public health, care coordination organizations.

State Designated Entity (SDE) means the entity designated by the NYS DOH to develop and oversee the implementation of the SHIN-NY, which entity shall be the New York eHealth Collaborative, Inc. (NYeC).
1. OVERSIGHT

This section sets forth the process for monitoring a QE’s compliance with applicable State, Federal and local law and the Certification Requirements. The mechanisms for detection by the Oversight Entity of Non-Compliance include: (a) a QE’s obligation to report Non-Compliance, whether discovered in connection with a self-audit or otherwise; (b) a complaints process through which stakeholders in the SHIN-NY, including Participants, can file complaints and/or reports of Non-Compliance; and (c) an external audit process through which the Oversight Entity monitors and audits a QE’s compliance with applicable State, Federal and local law and the Certification Requirements. This section also sets forth a process for investigating any potential Non-Compliance by a QE with applicable State, Federal and local law or the Certification Requirements. The mechanisms for investigating potential Non-Compliance include Internal Investigation by the QE and/or external investigation by the Oversight Entity. All Non-Compliance, regardless of the method of detection, will be addressed by the Oversight Entity who will gather the information necessary for determining the appropriate remedy.

1.1. QE Reporting.

1.1.1. Self-Audit.

1.1.1.1. Each QE shall perform, or shall cause a third-party to perform, an audit (a “Self-Audit”) in order to verify its compliance with applicable State, Federal and local law and the Certification Requirements at least once per year, as required by the Oversight Entity and as stated in the SHIN-NY Policy Standards Privacy & Security Policies and Procedures Section 6: Audit: Sub-section 6.2.3. The scope of the Self-Audit shall include at a minimum a review of QE’s compliance with applicable State, Federal and local law and the Certification Requirements.

COMMENT: The Oversight Entity shall prepare the self-audit check list for the QEs with input from key stakeholders.

1.1.2. Internal Investigation.

1.1.2.1. If a QE becomes aware of potential Non-Compliance or receives notice of a Non-Compliance Complaint (as hereinafter defined), the QE shall conduct an internal investigation (an “Internal Investigation”) of such complaint to determine whether Non-Compliance has occurred.

1.1.2.2. The QE shall begin the Internal Investigation within 30 days after becoming aware of potential Non-Compliance or receiving notice of a Non-Compliance Complaint.

1.1.2.3. The QE shall complete the Internal Investigation as soon as reasonably practicable but in any event no later than 60 days after becoming aware of potential Non-Compliance or receiving notice of a Non-Compliance Complaint.

1.1.3. Reporting.

1.1.3.1. Following an Internal Investigation conducted pursuant to Section 1.1.2, each QE shall report to the Oversight Entity in writing the existence of any Non-Compliance immediately after the QE determines that Non-Compliance has occurred. The report (the “Non-Compliance Report”) shall describe the Non-Compliance and any harmful effects known to the QE (including a list of Participants harmed, if any) resulting from Non-Compliance. NOTE: the Oversight Entity will develop a process for determining
the types of non-compliance that warrant investigation and reporting and will seek input from key stakeholders on that process.

1.1.3.2. If instructed by the Oversight Entity to perform an Internal Investigation pursuant to Section 1.3.1 the QE shall report the results of such investigation to the Oversight Entity. If the QE did not detect Non-Compliance as a result of such Internal Investigation, QE shall provide to the Oversight Entity a statement that no Non-Compliance was detected and a summary of the Internal Investigation conducted outlining the investigation findings.

1.1.3.3. Except as set forth in Section 1.1.3.1 and 1.1.3.2, above, the QE may, but shall not be obligated to, share the results of any other Self-Audit or Internal Investigation with the Oversight Entity.

1.2. Complaints Process.

1.2.1. Each QE shall develop and implement policies and procedures for receiving, investigating and responding to complaints from stakeholders in the SHIN-NY, including Participants.

1.2.2. Any stakeholder in the SHIN-NY, including any Participant, may file a complaint of any suspected Non-Compliance with the QE or the Oversight Entity. The complaint (the "Non-Compliance Complaint") must be in writing and must include the following information if known: (a) the suspected Non-Compliance, (b) the acts or omissions believed to constitute Non-Compliance; (c) the name of the QE involved; (d) the name of the Participant involved, if any; (e) all dates related to the suspected Non-Compliance; (f) all locations related to the suspected Non-Compliance, if any.

1.2.3. A Non-Compliance Complaint related to QE/QE Participant must be filed within 180 days from the date the complainant knew or should have known that non-compliance occurred for the Non-Compliance Complaint to be subject to investigation under this Policy.

1.2.4. If a Non-Compliance Complaint related to QE/QE Participant is filed with the QE, the QE shall conduct an Internal Investigation in accordance with Section 1.1.2. If a Non-Compliance Complaint is filed with the Oversight Entity, the Oversight Entity shall follow the procedures set forth in Section 1.3.

COMMENT: If a complaint is not a Non-Compliance issue, it shall be governed by the QE’s internal complaint handling procedures.

1.3. External Investigation Process.

1.3.1. Upon receipt of a Non-Compliance Complaint, the Oversight Entity shall either (a) conduct an investigation (an "External Investigation") of such Non-Compliance Complaint or (b) refer such Non-Compliance Complaint to the applicable QE if the Oversight Entity determines, based on a preliminary review of the facts, that an Internal Investigation by the QE is necessary or appropriate. If the Oversight Entity refers the Non-Compliance Complaint to the QE, the QE shall conduct an Internal Investigation pursuant to Section 1.1.2 and provide any reports or notices required by Section 1.1.3. NOTE: The factors to be considered by the Oversight Entity when determining whether an External Investigation or an Internal Investigation by the QE is necessary or appropriate include, but are not limited to, the following: nature of the Non-Compliance Complaint, history of complaints similar to the Non-Compliance Complaint with respect to the applicable QE, number of QEs
1.3.2. Upon receipt of a Non-Compliance Report from a QE, if the Oversight Entity, in its sole discretion, determines, based on a preliminary review of the facts, that a Non-Compliance was likely to have occurred, the Oversight Entity shall either (a) conduct an External Investigation of such Non-Compliance Report, if the Oversight Entity reasonably determines that an External Investigation is necessary or appropriate or (b) document a Report of Findings in accordance with Section 1.3.5 for the determination of remedies in accordance with Section 2.

1.3.3. If the Oversight Entity determines that it will conduct an External Investigation, the Oversight Entity shall begin the External Investigation within 30 days after the receipt of a Non-Compliance Report or a Non-Compliance Complaint. To begin the External Investigation, the Oversight Entity shall notify (a) in the case of a Non-Compliance Report, the QE who filed the Non-Compliance Report or (b) in the case of a Non-Compliance Complaint, the complainant and the QE named in the Non-Compliance Complaint. The notice ("Investigation Notice") shall include a summary of the intended External Investigation, including any requests for additional information from the QE, the Participant and/or the complainant.

1.3.4. Each QE requires its Participants to cooperate with the Oversight Entity in connection with any External Investigation, including by providing to the Oversight Entity the information requested in the Investigation Notice and access to its books, records, accounts and other sources of information related to the scope of the External Investigation.

1.3.5. The Oversight Entity shall document its findings ("Report of Findings") in response to the receipt of a Non-Compliance Report or Non-Compliance Complaint and share such Report of Findings with the applicable QE, the SDE and, if the Oversight Entity that performed the External Audit is a third-party designee of NYS DOH, it will also be shared with NYS DOH. Such Report of Findings shall include, at a minimum, the following: (a) the alleged non-compliance as related to applicable State, Federal and local law and/or the Certification Requirements, (b) events giving rise to the alleged non-compliance, (c) method of discovery of the non-compliance, i.e., self-audit, complaint, etc. (d) summary of the external investigation or an explanation if one was not conducted, if applicable, and (e) a summary of the findings.

1.3.6. The Oversight Entity shall finalize the Report of Findings as soon as reasonably practicable but in any event no later than 60 days after the receipt of a Non-Compliance Report or a Non-Compliance Complaint.

1.4. External Audit Process.

1.4.1. The Oversight Entity will, in conjunction with its ongoing monitoring, conduct periodic assessments of specific State, Federal and local law and Certification Requirements and if the Oversight Entity that performed the assessments is a third-party designee of NYS DOH, will submit a report of findings and recommendations for potential follow up actions to NYS DOH.

1.4.2. External Audits shall be performed during regular business hours upon reasonable notice to the QE of no less than 10 business days. External Audits may be performed no more than once per year per QE, unless there is reason to believe that the QE is in non-compliance with applicable State, Federal and local law or one or more of the Certification Requirements.
1.4.3. The QE requires its Participants to cooperate with the Oversight Entity in connection with any External Audit, including by providing to the Oversight Entity access to its books, records, accounts and other sources of information related to the scope of the External Audit.

1.4.4. The Oversight Entity shall document the results of any External Audit in a written report ("External Audit Report") and share such External Audit Report with the applicable QE, the SDE and, if the Oversight Entity that performed the External Audit is a third-party designee of NYS DOH, will submit the report to NYS DOH. Such External Audit Report shall include, at a minimum, the following: (a) scope of the External Audit performed, (b) a summary of the findings including any non-compliance related to applicable State, Federal and local law or the Certification Requirements and the events giving rise to non-compliance if applicable, (c) the method of discovery of non-compliance and (d) a root cause analysis if non-compliance occurred.

1.4.5. The Oversight Entity shall finalize the External Audit Report as soon as reasonably practicable but in any event no later than 60 days after providing notice to the QE of its intention to perform an External Audit.

1.5. Record Retention.

1.5.1. Each QE shall retain records relating to this Section 1 (including the results of all Self-Audits and all Non-Compliance Reports) for a period of at least six years.

1.5.2. The Oversight Entity shall retain records relating to this Section 1 (including all Investigation Notices, Reports of Findings, External Audit Reports, Non-Compliance Reports, Non-Compliance Complaints) for a period of at least six years.

2. ENFORCEMENT

The Remedy imposed on a QE shall be based on the nature and severity of Non-Compliance as determined by the Oversight Entity.

2.1. Types of Remedies. Remedies established by the Oversight Entity shall be commensurate with the nature of Non-Compliance.

2.1.1. Remedies that may be imposed by the Oversight Entity shall include, but are not limited to: (a) a written warning setting forth non-compliance related to applicable State, Federal and local law or the Certification Requirement(s), (b) corrective action requiring the QE to take affirmative steps to cure the non-compliance with milestones and dates by which each milestone must be completed, (c) monitoring requiring the QE to undergo a period of monitoring to assure continued compliance with specific State, Federal and local law and/or Certification Requirements, (d) temporary restriction of QE participation in the SHIN-NY, (e) permanent restriction of QE participation in the SHIN-NY and (f) imposition of fines only in instances in which one or more of the above remedies has previously been imposed and there is clear need for additional remedies beyond (a) through (e) above that fit the severity of non-compliance.

2.2. Determining Applicable Enforcement Action.

2.2.1. The Oversight Entity shall consider the following factors in determining the appropriate Remedy to be applied.
2.2.1.1. Nature and extent of Non-Compliance and the extent of actual or potential harm to any stakeholder in the SHIN-NY resulting from Non-Compliance.

2.2.1.2. QE’s level of culpability, i.e., was the nature of the circumstances leading to or causing Non-Compliance inadvertent, negligent, reckless, or intentional.

2.2.1.3. Any corrective action or other steps taken by the QE to respond to the events leading up to or constituting Non-Compliance, including performance of an Internal Investigation by the QE, the QE’s cooperation in the External Investigation or External Audit, as applicable.

2.2.1.4. QE’s history of prior compliance.

2.2.1.5. Impact of the Remedy on Participants.

2.2.1.6. Such other factors as the Oversight Entity may deem appropriate.

**COMMENT:** The Oversight Entity shall make available its ranking scale for determining the non-compliance level that will influence the type of remedy to be applied.

2.3. Application of Remedies

2.3.1. Upon review of the Report of Findings or External Audit Report, as applicable, the Oversight Entity shall determine the applicable Remedy to be imposed on the QE in accordance with the guidelines set forth in this Section 2.1.

2.3.2. The Oversight Entity shall determine the applicable Remedy within, at a minimum 15 calendar days after the Report of Findings or External Audit Report, as applicable, is finalized.

2.3.3. The Oversight Entity shall maintain documentation of the process that was used for determining the applicable Remedy, including documentation of all factors considered.

2.3.4. The Oversight Entity shall provide written notice (“Remedy Notice”) of the Remedy to the QE within 3 business days after determination of the Remedy. The Remedy Notice must set forth (a) a reference to the applicable Report of Findings or External Audit Report, (b) the Remedy, (c) any applicable timeframes, (d) the factors considered when determining the Remedy and (e) the process for appealing the determination of the Remedy.

2.3.5. The Oversight Entity may not impose a Remedy more than 5 business days after receiving the audit report of Non-Compliance.

2.4. Appeals

2.4.1. The QE shall have the right to appeal the Oversight Entity’s imposition of a Remedy no later than 60 days after receipt by the QE of the Remedy Notice. The QE shall provide written notice (“Appeal Notice”) to the Appeals Committee of its intention to appeal the imposed Remedy. The Appeal Notice must set forth (a) a reference to the applicable Remedy Notice and (b) the QE’s reason for appealing the imposed Remedy.

2.4.2. Subject to Section 2.4.4, within 3 business days after receipt of the Appeal Notice, the Appeals Committee shall provide notice to the Oversight Entity and the QE setting forth the
date for the appeal hearing, which date shall be no later than 30 calendar days after receipt of the Appeal Notice.

2.4.3. At the appeals hearing, the Oversight Entity and the QE shall each have an opportunity to present to the Appeals Committee an argument for or against the imposed Remedy. If the Appeals Committee determines that there are no grounds for appeal, the Appeals Committee will provide notice to the Oversight Entity and the QE of dismissal of the appeal. Such dismissal notice shall set forth (a) a reference to the applicable Appeal Notice and (b) the reason for dismissing the appeal.

2.4.4. The Appeals Committee shall maintain documentation of the appeal hearing.

2.4.5. No later than 15 business days after the appeal hearing, the Appeals Committee shall provide written notice (“Appeal Decision”) to the Oversight Entity and the QE of its decision regarding the imposed Remedy.

2.5. Documentation

2.5.1. The Oversight Entity shall retain records relating to this Section 2 (including all Remedy Notices and all documentation relating to determination of Remedies) for at least six years after a final determination is made with respect to each Remedy.

2.5.2. The Appeals Committee shall retain records relating to this Section 2 (including all Appeals Notices, Appeals Decisions and all documentation relating to the appeals hearing) for at least six years after a final determination is made with respect to each appeal.

OVERARCHING POLICY COMMENTS

Consideration will be made for cost of oversight and enforcement activities and the allocation of those costs, balanced by the severity of the Non-Compliance. Non-compliance that risks the integrity and security of the data will be more stringently viewed and enforced by the Oversight Entity.

Cost is also a factor for consideration related to the complaint process for handling and investigating Non-Compliance that will be influenced by the Oversight Entity’s enforcement (application of remedies).
Qualified Entity (QE) 
Minimum Technical Requirements

Version 1.2
REVISED June 2014

AS DEVELOPED THROUGH THE STATEWIDE HEALTH INFORMATION NETWORK OF NEW YORK (SHIN-NY) POLICY STANDARDS
# Table of Contents

- **INTRODUCTION** .................................................................................................................. 3
- **MINIMUM TECHNICAL STANDARDS** .................................................................................. 4

## 1. PATIENT RECORD LOOKUP ..................................................................................................... 6
   - 1.1 *User Requirements* ........................................................................................................ 6
   - 1.2 *QE Capabilities* ............................................................................................................ 6
   - 1.3 *Shin-Ny Service Levels* .................................................................................................. 7

## 2. SECURE MESSAGING ............................................................................................................... 8
   - 2.1 *User Requirements* ........................................................................................................ 8
   - 2.2 *QE Capabilities* ............................................................................................................ 8
   - 2.3 *Shin-Ny Service Levels* .................................................................................................. 9

## 3. CONSENT MANAGEMENT ......................................................................................................... 10
   - 3.1 *User Requirements* ........................................................................................................ 10
   - 3.2 *QE Capabilities* ............................................................................................................ 10
   - 3.3 *Shin-Ny Service Levels* .................................................................................................. 10

## 4. NOTIFICATIONS (ALERTS) .................................................................................................... 12
   - 4.1 *User Requirements* ........................................................................................................ 12
   - 4.2 *QE Capabilities* ............................................................................................................ 12
   - 4.3 *Shin-Ny Service Levels* .................................................................................................. 12

## 5. IDENTITY MANAGEMENT AND SECURITY ........................................................................... 14
   - 5.1 *User Requirements* ........................................................................................................ 14
   - 5.2 *QE Capabilities* ............................................................................................................ 14
   - 5.3 *Shin-Ny Service Levels* .................................................................................................. 14

## 6. PROVIDER AND PUBLIC HEALTH CLINICAL VIEWER ..................................................... 15
   - 6.1 *User Requirements* ........................................................................................................ 15
   - 6.2 *QE Capabilities* ............................................................................................................ 15
   - 6.3 *Shin-Ny Service Levels* .................................................................................................. 15
7. PUBLIC HEALTH INTEGRATION ........................................................................ 16

7.1 USER REQUIREMENTS .............................................................................. 16
7.2 QE CAPABILITIES ...................................................................................... 16
7.3 SHIN-NY SERVICE LEVELS ....................................................................... 16

8. RESULTS DELIVERY .................................................................................... 17

8.1 USER REQUIREMENTS .............................................................................. 17
8.2 QE CAPABILITIES ...................................................................................... 17
8.3 SHIN-NY SERVICE LEVELS ....................................................................... 17
Introduction

This document was developed through the SHIN-NY Policy Standards (SPS), to document baseline minimum technical requirements that organizations must fulfill to be considered New York State Qualified Entities (QEs). The requirements will be evaluated as part of the Certification Process by the Certification Body (as such terms are defined in the Qualified Entity (QE) Organizational Characteristics Requirements (as amended from time-to-time, the “Organizational Characteristics”) that will be under contract with State’s Designated Entity, under agreement and in conjunction with the New York State Department of Health (NYS DOH). All capitalized terms used and not defined herein shall have the respective meanings given to such terms in the Privacy and Security Policies and Procedures for QEs and their Participants in New York State (as amended from time-to-time, the “Policies and Procedures”).

Minimum Technical Requirements are the essential capabilities described herein that each Qualified Entity must be capable of providing in an acceptably common format by a given date, as certified by the Certification Body. The minimum technical requirements are defined according to how a user at a provider, payer or public health authority organization would experience the minimum technical requirements as provided by a QE.
Minimum Technical Requirements

While it is envisioned that Qualified Entities will be certified based on their ability to deliver or cause to be delivered the minimum technical requirements described in this document, it is important to distinguish which minimum technical requirements will be enabled cross-community, statewide or even nationwide, and which will be enabled to serve only local QE Participants. Minimum technical requirements are also distinguished by how they are anticipated to be enabled by a QE (e.g., QE-provided tools, through integration with third-party software applications such as EMRs or EHRs) and by the potential level of integration required with SHIN-NY defined or potential future capabilities. It is acknowledged that Qualified Entities may cause to be delivered the minimum technical requirements described in this document, it is important to distinguish which minimum technical requirements identified below as “Cross-Community” by executing a Qualified Entity Participation Agreement with state designated entity pursuant to which the state designated entity shall provide such minimum technical requirements identified below as “Cross-Community.” The following table summarizes these distinctions in an attempt to provide context for the lists of service-specific requirements that follow.

<table>
<thead>
<tr>
<th>Service</th>
<th>Local / Cross-Community</th>
<th>QE Implementation Method(s) / Requirements</th>
<th>Potential SHIN-NY Component</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Record Lookup</td>
<td>Cross-Community</td>
<td>• Local MPI &lt;br&gt; • Clinical Viewer &lt;br&gt; • Interfaces to 3rd Party Software (incl. EMR/EHR)</td>
<td>SHIN-NY MPI Functionalities Forthcoming</td>
<td>• Opportunity for access to data from more sources with statewide MPI</td>
</tr>
<tr>
<td>Secure Messaging</td>
<td>Cross-Community</td>
<td>• Provider Directory / Master Clinician Index &lt;br&gt; • Clinical Viewer &lt;br&gt; • Interfaces to 3rd Party Software &lt;br&gt; • Email (Direct)</td>
<td>Statewide Provider Directory / Master Clinician Index</td>
<td>• Direct Project standards and protocols &lt;br&gt; • Opportunity for greater efficiencies with statewide Provider Index / Master Clinician Index</td>
</tr>
<tr>
<td>Consent Management</td>
<td>Local</td>
<td>• Support service and / or online tool provided by QE &lt;br&gt; • Interfaces to 3rd Party Software</td>
<td>Managed to allow access to patient records across the state</td>
<td>• Statewide policy &lt;br&gt; • Local implementation details left to QE &lt;br&gt; • “Break the glass” events reported cross-community as part of Patient Record Lookup service</td>
</tr>
<tr>
<td>Notifications (Alerts)</td>
<td>Local</td>
<td>Support service and / or online tool provided by QE</td>
<td>May evolve to statewide; in the meantime, QEs must allow users of other QEs to subscribe to events occurring in the local QE on the same terms and under the same processes as users of the local QE, including executing any agreements required by the local QE</td>
<td>• QEs communicate requests for cross-community notifications to other QEs (for border providers, patients travelling for treatment, etc.) &lt;br&gt; • Local QE follows its standard local processes to accept a subscription from the user of another QE</td>
</tr>
<tr>
<td>Identity Management &amp; Security</td>
<td>Local</td>
<td>Self-service and administrative / help desk support</td>
<td>Two Factor Authentication services available statewide for use by any QE</td>
<td>• Statewide policy &lt;br&gt; • Opportunity for cost-sharing with statewide or shared services for Two Factor Authentication</td>
</tr>
<tr>
<td>Provider and Public Health</td>
<td>Local</td>
<td>Local implementation details and features left to QE</td>
<td></td>
<td>• Minimum capabilities specified statewide</td>
</tr>
<tr>
<td>Clinical Viewer</td>
<td>Local</td>
<td>Local implementation details and features left to QE</td>
<td>In conformance with public health use cases (TBD)</td>
<td>• Statewide policy and standards</td>
</tr>
<tr>
<td>Public Health Integration</td>
<td>Local (Statewide standards)</td>
<td>Local implementation details and features left to QE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Results Delivery</td>
<td>Local</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Presentation in Clinical Viewer</td>
<td>• Interfaces to 3rd Party Software at QE’s discretion</td>
<td>• Lab and radiology at minimum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Email (Direct)</td>
<td>• Lab and radiology at minimum</td>
<td>• Delivery to ordering provider, at a minimum</td>
<td></td>
</tr>
</tbody>
</table>
1. Patient Record Lookup

Patient record lookup provides Authorized Users with the ability to search for existing patient records within the local QE, across all other QEs statewide and eventually, across a broader nationwide network when available and connected to the SHIN-NY. This service will enable the matching of patient records at a local level using patient specific demographic information or local facility medical record numbers (MRNs). A local master person index (MPI) will be managed by the QE to associate records within the QE and to match patient records available from other QEs statewide using the SHIN-NY supported statewide MPI. This service will provide information to providers accessing the SHIN-NY via third party software, QE-provided clinical viewers and patient portals, public health applications or other validated end-points connected to a QE.

1.1 User Requirements

Through usage of services available from the QE, an Authorized User must be able to:

1.1.1 Search by patient demographics or using a known patient identifier for a patient statewide across all QEs known to the QE from which the search originates

1.1.1.1 Patient demographics search must at minimum support entry and search by name, date of birth and gender; not all data elements are necessarily required, and additional data elements can be accepted, at the discretion of the originating QE

1.1.1.2 Known patient identifier search must support entry and search using a facility name medical record number (or equivalent, i.e., member number for a payer Participant) pair

1.1.2 Search across all SHIN-NY connections without knowledge of where data may exist, including but not limited to all connected New York State QEs and any other connected national or regional networks such as the nationwide HealtheWay

1.1.2.1 At its option, the originating QE can search and return its own data before passing the query to the SHIN-NY for resolution against the consolidated statewide MPI, but the Authorized User cannot be required to enter a second search or take another action in order to search against the consolidated statewide MPI; even if the search is performed in two steps, the statewide search must be conducted without further Authorized User interaction, except at the Authorized User’s option, as described below

1.1.2.2 At its option, the originating QE may offer a local search option controlled by the Authorized User (e.g., through separate search buttons or a drop down box with separate options for local or statewide/national search), as long as either or multiple forms of query can be launched with one click / action (and not force the Authorized User to search locally before executing the broader search)

1.1.3 Search from within a QE’s clinical viewer

1.1.4 Search from within third party software supported by the QE providing that all of the following conditions are met:

1.1.4.1 The third party software interface meets the standards and requirements of the QE and SHIN-NY for patient lookup; proprietary interfaces are supported at the QE’s discretion

1.1.4.2 QE Authorized Users request testing and supporting a query from the third party software, and testing and supporting the query interface is economically feasible and sustainable for the QE; there is no requirement to support “all comers;” third party software interfaces are supported at the QE’s discretion

1.1.5 After selecting a patient, retrieve records from all desired data sources known to the local QE

1.1.6 Indicate that a patient lookup request is a request to “break the glass” due to an emergency condition as defined in 1.2.3 of SHIN-NY Policies and Procedures, in order to gain access to records for which consent to access has not previously been given by the patient

1.2 QE Capabilities

QE service capabilities must:

1.2.1 Service queries by Authorized Users as described above
1.2.2 Be capable of receiving a query from the SHIN-NY for a specific MPI and service it by returning a CCD or other information to the SHIN-NY, as defined and approved pursuant to the Statewide Collaboration Process.

1.2.3 Be capable of notifying querying QE that no match was found; at its discretion, querying QE can display, log or dismiss such "no match" responses.

1.2.4 Be made available to all validated Authorized Users connected to a QE via clinical viewer, third party software or patient portal.

1.2.5 Conform to standards and specifications established by the SCP.

1.2.6 Support SHIN-NY access control specifications and identity management requirements established pursuant to the Statewide Collaboration Process and by New York State regulation.

1.2.7 Be subject to patient consent to access data cross-community, such that the originating QE confirms that the patient has given consent for the querying provider to access the patient’s data.

   1.2.7.1 Provide an exception to ordinary consent restrictions when the querying provider requests to “break the glass” due to an emergency condition.

   1.2.7.2 Provide an exception to ordinary consent restrictions when the querying Authorized User is a public health user accessing a patient’s data under applicable Public Health uses as defined by SHIN-NY Policies and Procedures and state law.

1.2.8 Log all patient record lookup requests sent and received as required by New York State regulation and the SHIN-NY Policy Standards, with audit data specified pursuant to the Statewide Collaboration Process.

   1.2.8.1 Including separately identifying requests to “break the glass” on patient consent restrictions in the case of an emergency condition.

1.3 SHIN-NY Service Levels

The end-to-end service experience must include:

1.3.1 Responding QEs must be able to send a response within a set length of time from receiving a query for a set percentage of the transactions received, as defined and approved pursuant to the Statewide Collaboration Process.

1.3.2 Records are returned to the originating QE within a set length of time from an Authorized User request, or at the end of a tunable timeout period set by the originating QE, as defined and approved pursuant to the Statewide Collaboration Process.

1.3.3 Conformance to service levels for reliability and availability established by the SCP.
2. **Secure Messaging**

Secure messaging services provide Authorized Users with the ability to send peer-to-peer messages between two trusted providers. At this time, the Direct Project ([http://directproject.org/](http://directproject.org/)) provides the de facto standard and state of the art practice and protocol for such messaging, which it describes as “the push of health information from a sender to a known receiver, similar to how an email or fax is pushed from one endpoint to another.” Requirements for this service are described in the Direct Project context, and Direct Project standards and protocols provide the minimum and required method for cross-community messaging at this time. The standard for secure messaging is subject to change in the future as other protocols or methods emerge to overtake Direct.

### 2.1 User Requirements

Through usage of services available from the QE, an Authorized User must be able to:

2.1.1 Generate messages and/or documents to be sent as message attachments from within supported third party software or QE clinical viewer

2.1.2 Send messages, with or without attached documents, directly and securely to an Authorized User or list of users

2.1.3 Look up intended recipients in a Provider Directory / Master Clinician Index provided by the SHIN-NY or approved for use pursuant to the Statewide Collaboration Process
   - 2.1.3.1 For electronic addressing
   - 2.1.3.2 Enabling the Authorized User to select one or more recipient to automatically embed routing information in a message

2.1.4 Specify an electronic address for receiving messages, including a SHIN-NY Direct inbox hosted by a third party

2.1.5 Request and receive messages and/or documents from other QEs for delivery to an electronic address provided in the request that can be authenticated by the sender in a Provider Directory / Master Clinician Index or through another method approved pursuant to the Statewide Collaboration Process
   - 2.1.5.1 Responding QE must be able to determine that the address provided is valid and securely associated with the requesting provider

2.1.6 Receive notifications of undeliverable messages, as defined and approved pursuant to the Statewide Collaboration Process

2.1.7 Receive and decrypt messages to the provider from any secure communication source supported by the Direct Project standards.

### 2.2 QE Capabilities

QE service capabilities must:

2.2.1 Make available a system to send secure messages for those providers who do not have access to secure messaging through other applications (such as an EMR/EHR)

2.2.2 Conform to standards and specifications established by the SCP (minimally, Direct Project protocols at this time)

2.2.3 Encrypt / decrypt messages according to standards defined by the SCP

2.2.4 Deliver messages without examining content

2.2.5 Verify that incoming messages are properly signed by an appropriate certificate authority

2.2.6 Generate a return receipt or other form of acknowledgement if requested by the sender in an automated fashion (e.g., as a feature of commercial email software, rather than in the text of a message)

2.2.7 Log all messages sent and received as required by New York State regulation and the SHIN-NY Policy Standards, with audit data specified pursuant to the SCP
2.3 SHIN-NY Service Levels

The end-to-end service experience must include:

2.3.1 Receiving QE must notify the sender of a failure to deliver a message within a set length of time from receipt of the message at the QE for a set percentage of failures, as defined and approved pursuant to the Statewide Collaboration Process.

2.3.2 Conformance to service levels for reliability and availability established by the SCP.
3 Consent Management

Consent management services provide the ability to track patient consent according to New York State law and other requirements defined pursuant to the Statewide Collaboration Process for the SHIN-NY. New York and SHIN-NY consent policy is defined as “consent to access” patient records. Access must be explicitly granted to providers in writing by patients “opting in” to data access at the entity level (hospital, provider practice, individual practitioner, etc.). Written consent is collected by each provider and communicated to one or more QEs. QEs maintain a local cross reference of patient/provider consent that can be checked before releasing any information, including information that identifies which providers have generated patient records to a provider or another QE. QEs are not responsible for verifying consent authorization for information sent via 1:1 exchange including when acting solely as delivery and routing agent for Direct messages. The Authorized User is responsible for ensuring 1:1 exchange messages are appropriate under implied or written consent as required by law.

3.1 User Requirements

Through usage of services available from the QE, an Authorized User must be able to:

3.1.1 Record consent to access patient data, as explicitly authorized by a patient
3.1.2 Record denial of consent
3.1.3 Record consent to access on an emergency basis only (“break the glass”)
3.1.4 Review and modify consent status on behalf of a patient using an online interface provided by the QE
3.1.5 Manage consent permissions and restrictions from within third party software with consent management capabilities, with an interface supported by the QE, providing that all of the following conditions are met:
   3.1.5.1 The third party software interface meets the standards and requirements of the QE and SHIN-NY for consent management; proprietary interfaces are supported at the QE’s discretion
   3.1.5.2 QE Authorized Users request testing and supporting a consent management interface from the third party software, and testing and supporting the query interface is economically feasible and sustainable for the QE; there is no requirement to support “all comers;” third party software interfaces are supported at the QE’s discretion
3.1.6 Make consent inquiries to verify the consent status for a given patient for that provider organization using the same search criteria enabled by the Patient Record Lookup service
   3.1.6.1 For current consents
   3.1.6.2 At a point in time, by providing a date and time in addition to other search criteria
3.1.7 Gain access without patient affirmative consent by “breaking the glass” in emergency condition situations as defined by SHIN-NY Policies and Procedures
   3.1.7.1 Specifically for Public Health Users, gain access without patient affirmative consent for applicable Public Health uses as defined in SHIN-NY Policies and Procedures and state law.

3.2 QE Capabilities

QE service capabilities must:

3.2.1 Maintain a system for adding, modifying and reviewing the status of an individual patient consent
   3.2.1.1 Timestamp and maintain a history of all changes to consents, including initial creation, updates and revocations
   3.2.1.2 Consent records must not be deleted; consent history must be maintained in order to establish consent in place at a given point in time
3.2.2 System must conform to all SHIN-NY Policy Standards regarding consent management
3.2.3 Adequately log and communicate “break the glass” events in patient record lookup requests, via notification messages or through other methods as defined in the SPG
3.2.4 QE must provide a method for an Authorized User to verify the consent status of a patient
3.3 SHIN-NY Service Levels

The end-to-end service experience must include:

3.4.1 Conformance to service levels for reliability and availability established by the SCP
4 Notifications (Alerts)

Notification services allow Authorized Users to establish subscriptions to pre-defined events and receive notifications when those events occur. These services are subject to consent requirements established pursuant to the Statewide Collaboration Process.

4.1 User Requirements

Through usage of services available from the QE, an Authorized User must be able to:

4.1.1 Subscribe to notification feeds related to the following events
   4.1.1.1 ER admit
   4.1.1.2 Inpatient admit
   4.1.1.3 Inpatient discharge

4.1.2 Receive notifications related to patients for which the Authorized User has subscribed at an electronic address and in a format (provided at the time of subscription), including at minimum, as either:
   4.1.2.1 Secure messaging
   4.1.2.2 HL7 formatted documents and data

4.1.3 Review all active subscriptions

4.1.4 Unsubscribe from notification feeds

4.2 QE Capabilities

QE service capabilities must:

4.2.1 Provide a mechanism for entering and maintaining subscriptions to notifications for a pre-set list of notifiable events such as admissions and discharges
   4.2.1.1 Mechanisms may include self-service data entry using an electronic process provided by the QE or an administrative service whereby QE staff enters subscriptions on behalf of subscribing providers (subscribers)

4.2.2 “Listen for” and detect notifiable events from within HL7, PIX or other standard message types specified by the SCP

4.2.3 Deliver notifications to subscribers when data required to detect a notifiable event is transmitted to the QE by a data provider

4.2.4 Facilitate subscription requests received from a provider from another community when the provider wishes to subscribe to notifications from provider organizations served by the local QE (subject to the subscription policies and processes of the local QE)

4.2.5 Report notifications that are unable to be sent to subscriber (subscriber not found) to a monitored exception queue at the QE

4.2.6 Log all notifications sent to and received from the SHIN-NY subscription listener or directly from / to another QE with audit data specified pursuant to the SCP

4.2.7 Conform to standards and specifications established by the SCP

4.2.8 Deliver notifications in accordance with all consent requirements of the SHIN-NY Policy Standards

4.2.9 Log all notifications sent and received as result of a subscription as required by New York State regulation and the SHIN-NY Policy Standards, with audit data to be specified pursuant to the SCP

4.3 SHIN-NY Service Levels

The end-to-end service experience must include:

4.3.1 Ability to send messages within a set length of time from receiving messages from a source system, as defined and approved pursuant to the Statewide Collaboration Process
4.3.1.1 QEs can modify this service level for a specific Participant via custom contractual agreement

4.3.2 Conformance to service levels for reliability and availability established by the SCP

4.3.3 Ability to queue or otherwise store messages in the event of an outage

4.3.4 Ability to notify the SHIN-NY and / or other QEs in the event of an outage

4.3.5 Service subscription requests received from providers in another QE as if they were served by or customers / Authorized Users in the local QE
5 Identity Management and Security

Identity management and security services provide for secure access and ensure patient privacy through the authentication of all requests by individuals and organizations to view protected health information accessible through the QE.

5.1 User Requirements

Through usage of services available from the QE, an Authorized User must be able to:

5.1.1 Acquire credentials to use QE and SHIN-NY functions appropriate to the Authorized User’s authority
5.1.2 Set and change a password securely through a self-service capability without sharing an existing password in an unsecured manner
5.1.3 Receive assistance with authentication and access issues through a help desk or other attended services provided by the QE
5.1.4 Authenticate themselves once per session interacting with the QE through a standard approach
5.1.5 Re-authenticate themselves within the workflow of any functions requiring authentication more frequently than once per session, as defined in SHIN-NY Policies and Procedures (e.g., re-authentication on a per prescription basis for controlled substances)

5.2 QE Capabilities

QE service capabilities must:

5.2.1 Support multiple roles with configurable levels of access to SHIN-NY data, including access to limited document sets by role as developed by the SCP and defined in SHIN-NY Policies and Procedures
5.2.2 Allow authorized QE administrative Authorized Users the ability to add or delete roles on behalf of clinical Authorized Users
5.2.3 Allow authorized QE administrative Authorized Users the ability to modify access permissions for existing roles
5.2.4 Provide registration authority functions, including proving/verifying an Authorized User’s identity (identity proofing) prior to issuing credentials to use QE services and assigning unique addresses/Authorized User IDs for accounts, according to SHIN-NY Policies and Procedures
5.2.5 Meet authentication requirements as specified under 3.2.1 of the SHIN-NY Policies and Procedures
5.2.6 Pass and receive Security Assertion Markup Language (SAML) assertions cross-community as required once an Authorized User has been authenticated
5.2.7 Timeout Authorized User sessions and require re-authentication based on a maximum session duration according to standards established pursuant to the Statewide Collaboration Process
5.2.8 Include the ability to specify credential lifetime and revoke credentials at the expiration of their lifetime
5.2.9 Include the ability to immediately revoke credentials for any reason (e.g., loss, theft, voluntary or involuntary de-activation of Authorized User account, etc.) according to SHIN-NY Policies and Procedures
5.2.10 Log all successful and unsuccessful authentication attempts as required by SHIN-NY Policies and Procedures, with audit data specified pursuant to the Statewide Collaboration Process

5.3 SHIN-NY Service Levels

The end-to-end service experience must include:

5.3.1 Responding to requests for assistance with authentication and access issues within a reasonable timeframe established in the SHIN-NY Policies and Procedures
5.3.2 Immediately notifying and escalating known or suspected breaches of security according to the SHIN-NY Policy Standards.
6 Provider and Public Health Clinical Viewer

The QE will make available to qualified providers and public health authorities the ability to securely access individual patient records from all available local, statewide and other data sources accessible by the QE.

6.1 User Requirements

Through usage of services available from the QE, an Authorized User must be able to:

6.1.1 Search for records for an individual patient across all data sources (as defined by patient record lookup requirements) based on demographics, MRN or other patient identifying information

6.1.2 View a history of demographic and clinical records associated with a patient as provided and made available by participating data sources, including, to the extent QE has such data:
  6.1.2.1 Patient contact, demographics and insurance coverage
  6.1.2.2 Patient consent from within the local QE community, as required
  6.1.2.3 Encounter history and summaries
  6.1.2.4 Vital signs, diagnoses, allergies and medications
  6.1.2.5 Lab and radiology reports

6.1.3 View or gain access to patient records from all non-SHIN-NY sources (e.g., HealtheWay, Veterans Administration, etc.) with which the QE may also contract

6.2 QE Capabilities

QE service capabilities must:

6.2.1 Control access using role-based access control

6.2.2 Control access for all Authorized Users according to patient consent guidelines, applicable State, local and Federal laws and regulations, as developed pursuant to the Statewide Collaboration Process

6.3 SHIN-NY Service Levels

The end-to-end service experience must include:

6.3.1 Records are available within 5 minutes of being received by the QE when they can be auto-matched to the patient's MPI (i.e., using patient identifier or MRN identifier, without requiring manual MPI merging)

6.3.2 Conformance to service levels for reliability and availability as established by the SCP
7 Public Health Integration

Route required public health reporting information from primary sources to New York State and New York City Public Health Agency (PHA) designated aggregation points and return response messages from the respective PHAs to the originating provider.

7.1 User Requirements

Through usage of services available from the QE, an Authorized User must be able to:

7.1.1 Electronically report to the appropriate reporting entity as designated by the Department of Health for public health measures for which the QE has reporting capability as specified in 7.2.4

7.2 QE Capabilities

QE service capabilities must:

7.2.1 Send required public health reporting data according to standards, formats, specifications and quality assurance procedures specified by Local, State and Federal public health authorities

7.2.2 Enable public health role based queries of individual patient records, as defined and approved pursuant to the Statewide Collaboration Process

7.2.3 Log all public health reporting as required by the SHIN-NY Policy Standards, with audit data specified pursuant to the Statewide Collaboration Process

7.2.4 QE must provide at least one of the following public health reporting services to Authorized Users:

7.2.4.1 Immunizations – to NYS DOH and the New York City Department of Health and Mental Hygiene (NYC DOHMH)
7.2.4.2 Syndromic surveillance data – to NYS DOH and NYC DOHMH
7.2.4.3 Reportable laboratory results – to NYS DOH and NYC DOHMH
7.2.4.4 Cancer cases – to the NYS DOH Cancer registry (to be defined and approved pursuant to the Statewide Collaboration Process)
7.2.4.5 To support emergency preparedness and response efforts, specified data elements for connected facilities – to NYS DOH and NYC DOHMH, and receive requests and respond to a query related to a specific patient with demographic and location data in the case of an emergency and mass casualty event as defined and approved pursuant to the Statewide Collaboration Process
7.2.4.6 Newborn Bloodspot Screening (NBS) – electronic reporting of demographic and clinically relevant information (associated with newborn bloodspot samples) to NYS DOH and return of acknowledgements and electronic NBS lab results
7.2.4.7 For an authorized public health agency:

7.2.4.7.1 Automate the delivery of data on notifiable diseases/conditions, as developed in conjunction with NYS DOH and/or NYC DOHMH

7.3 SHIN-NY Service Levels

The end-to-end service experience must include:

7.3.1 Ability to queue or otherwise store reporting messages in the event of an outage for sending when either the sending QE or receiving public health end-point becomes available

7.3.2 Ability to pass through acknowledgements and verification messages as required by the public health reporting services to which the QE is connected.
8 Results Delivery
Deliver diagnostic results and reports back to ordering providers and others designated to receive results.

8.1 User Requirements
Through usage of services available from the QE, an Authorized User must be able to:

8.1.1 Receive diagnostic results and summary reports for, at minimum, laboratory and radiology tests from laboratories and diagnostic centers and facilities that have arranged to have the QE route results on their behalf

8.1.2 Receive results when the Authorized User is the ordering provider or has been listed in the order to receive copies of results

8.1.3 Receive results in one or more of the following methods stated as a preference by the Authorized User:
  8.1.3.1 Directly into the Authorized User’s EMR/EHR or other third party software
  8.1.3.2 For viewing in a QE’s clinical viewer
  8.1.3.3 As a Direct message at a designated address, including an email inbox

8.1.4 Methods and preferences other than viewing in the QE’s clinical viewer are supported providing that all of the following conditions are met:
  8.1.4.1 The third party software interface meets the standards and requirements of the QE and SHIN-NY for results delivery; proprietary interfaces are supported at the QE’s discretion
  8.1.4.2 QE Authorized Users request testing and supporting results delivery to the third party software or a Direct address, and testing and supporting interface is economically feasible and sustainable for the QE; there is no requirement to support “all comers;” third party software and Direct interfaces are supported at the QE’s discretion

8.2 QE Capabilities
QE service capabilities must:

8.2.1 Detect results from within HL7 messages received from source systems
8.2.2 Conform to standards and specifications established by the SCP

8.3 SHIN-NY Service Levels
The end-to-end service experience must include:

8.3.1 Results are routed to the specified end-point within a set length of time from receipt by the QE, as defined and approved pursuant to the Statewide Collaboration Process
  8.3.1.1 There is no guarantee of delivery to the end recipient in that timeframe, as delivery to the Authorized User may be a condition of additional arrangements within a QE or with an EMR/EHR vendor or other intermediary

8.3.2 Conformance to service levels for reliability and availability established by the SCP
Qualified Entity (QE)  
Member Facing Services 
Requirements

Version 1.2 
REVISED June 2014

AS DEVELOPED THROUGH THE STATEWIDE HEALTH INFORMATION NETWORK OF NEW YORK (SHIN-NY) POLICY STANDARDS
Table of Contents

INTRODUCTION .................................................................................................................. 3
MEMBER FACING SERVICES DEFINITION ........................................................................ 4

1. LEGAL & INFORMATION SHARING AGREEMENTS .............................................. 5
   1.1 FRAMEWORK ........................................................................................................ 5
   1.2 QE CERTIFICATION EVIDENCE REQUIREMENTS ........................................... 5
   1.3 CERTIFICATION TASKS AND QE EVALUATION STANDARDS ...................... 5
   1.4 ONGOING MONITORING AND AUDITS ............................................................ 5

2. MARKETING AND RECRUITMENT ........................................................................... 6
   2.1 FRAMEWORK ........................................................................................................ 6
   2.2 QE CERTIFICATION EVIDENCE REQUIREMENTS ........................................... 6
   2.3 CERTIFICATION TASKS AND QE EVALUATION STANDARDS ...................... 6
   2.4 ONGOING MONITORING AND AUDITS ............................................................ 6

3. SUPPORT FOR ADOPTION AND USAGE ............................................................ 8
   3.1 FRAMEWORK ........................................................................................................ 8
   3.2 QE CERTIFICATION EVIDENCE REQUIREMENTS ........................................... 8
   3.3 CERTIFICATION TASKS AND QE EVALUATION STANDARDS ...................... 8
   3.4 ONGOING MONITORING AND AUDITS ............................................................ 8

4. PARTICIPANT/AUTHORIZED USER TRAINING ........................................................ 9
   4.1 FRAMEWORK ........................................................................................................ 9
   4.2 QE CERTIFICATION EVIDENCE REQUIREMENTS ........................................... 9
   4.3 CERTIFICATION TASKS AND QE EVALUATION STANDARDS ...................... 9
   4.4 ONGOING MONITORING AND AUDITS ............................................................ 9

5. USER SUPPORT ....................................................................................................... 10
   5.1 FRAMEWORK ........................................................................................................ 10
   5.2 QE CERTIFICATION EVIDENCE REQUIREMENTS ........................................... 10
   5.3 CERTIFICATION TASKS AND QE EVALUATION STANDARDS ...................... 10
6. ALIGNING WITH STAKEHOLDER PRIORITIES .............................................. 11

6.1 Framework ............................................................................................................ 11
6.2 QE CERTIFICATION EVIDENCE REQUIREMENTS .............................................. 11
6.3 CERTIFICATION TASKS AND QE EVALUATION STANDARDS ......................... 11
6.4 ONGOING MONITORING AND AUDITS ................................................................. 11
Introduction

This document, developed through the statewide collaboration process, sets forth the defined minimum set of core Member Facing Services that QEs must implement and have available to all QE Participants. They include requirements for legal and information sharing agreements, providing marketing and recruitment strategies, adoption and usage support services, training for Participants and Authorized Users, user support services that focus on solving system access issues, a collaborative governance structure that supports Participant priorities and development of value added services that strengthen the SHIN-NY and serve to improve health care delivery for all New Yorkers.

The requirements set forth herein will be evaluated as part of the Certification Process by the Certification Body (as such terms are defined in the Qualified Entity (QE) Organizational Characteristics Requirements (as amended from time-to-time, the “Organizational Characteristics”) that will be under contract with the New York eHealth Collaborative, Inc. (NYeC), under agreement and in conjunction with the New York State Department of Health (NYS DOH). All capitalized terms used and not defined herein shall have the respective meanings given to such terms in the Privacy and Security Policies and Procedures for QEs and their Participants in New York State (as amended from time-to-time, the “Policies and Procedures”).
Member Facing Services Definition

Member Facing Services means facilitative services provided by the Qualified Entity that offer value to its participants and that ensure the secure exchange and use of clinical and other health information among physicians and other health care providers including but not limited to health plans, consumers, Public Health, health homes and social service organizations, to improve patient care. To qualify as a Qualified Entity, an entity must be capable of providing the Member Facing Services.
1. **Legal & Information Sharing Agreements**

Enter into Participant Agreements and/or other agreements (including but not limited to data sharing agreements, business associate agreements, and documents), if applicable, that (x) clarify the responsibilities of Participants and vendors in relation to the QE and (y) ensure exchange of information in a private and secure manner and for authorized purposes only.

1.1 **Framework**

These agreements shall include

1.1.1 Participant Agreements and/or other agreements (including but not limited to data sharing agreements, business associate agreements, and documents), if applicable, that clarify the responsibility of Participants and vendors in relation to the QE.

1.1.2 Participant Agreement and/or other agreements (including but not limited to data sharing agreements, business associate agreements, and documents), that ensure privacy and security of information exchange by Authorized Users that is consistent with the Policies and Procedures.

1.2 **QE certification evidence requirements**

QE's must:

1.2.1 Provide signed Participant Agreements and/or other agreements (including but not limited to data sharing agreements, business associate agreements, and documents), that include

   1.2.1.1 the requirements for participation in the SHIN-NY in either a separate addendum to the Participant Agreement or within the provisions of the Participant Agreement, and

   1.2.1.2 the requirements for conformance to service levels as specified in service level agreements

1.3 **Certification tasks and QE evaluation standards**

The Certification Body will be required to verify evidence provided by the QE including:

1.3.1 QE data sharing agreements that are complete and signed

1.3.2 Conformance to service levels for reliability and availability established by the SCP

1.4 **Ongoing monitoring and audits**

In addition to QE’s obligations under or in accordance with the **Oversight & Enforcement Policies and Procedures for QEs** (as amended from time-to-time, the “Oversight and Enforcement Policies”), QEs shall ensure that an ongoing monitoring process includes:

1.4.1 Self-Audits that include ongoing monitoring of state regulatory or policy changes or corporate changes in Participant status.

1.4.2 That QEs shall ensure that no data connections or Authorized User credentials are completed before signing legal and information sharing agreements with a Participant.

1.4.3 External Audits and monitoring by the Certification Body that confirms the validity of Participant Agreements and/or other agreements via review of a specific number of these Participant Agreements and/or other agreements as part of QE audit.
2. Marketing and Recruitment

Utilize evidence-based marketing and education techniques and tools to promote QE services and the benefits of participating in an HIE. Efforts should include implementation of recruitment and outreach strategies that increase participation in the QE and that include but are not limited to hospitals/health care systems; ambulatory health care settings; payers; health homes; Medicaid; public health; labs; community based social service organizations. Outreach to consumer/patient groups to increase their understanding and appropriate usage of HIE, and to gain their input on HIE, is also required, although they are not recruited as Participants in the QE.

2.1 Framework

The service should include recruitment and outreach strategies that:

2.1.1 Increase participation from all interested candidates that might qualify for participation in a QE in the SHIN-NY

2.1.2 Enhance patient understanding of the value of consenting

2.2 QE certification evidence requirements

QEs must:

2.2.1 Make available a copy of their QE Marketing and Recruitment Plan that includes:

2.2.1.1 recruitment and outreach strategies and targets

2.2.1.2 communications/education activities/plan

2.2.1.3 description of target audience(s) for recruitment

2.3 Certification tasks and QE evaluation standards

The Certification Body will be required to verify evidence provided by the QE including:

2.3.1 Existence of QE Marketing and Recruitment Plan for period of review.

2.3.2 Conformance of QE Marketing and Recruitment Plan to standards:

2.3.2.1 QE Marketing and Recruitment Plan describes the QE approach to promoting HIE services and benefits and outlines measures for achieving increased numbers and diversity of Participants.

2.3.2.2 Includes communication and education strategies for both providers and patients that are designed to foster trust and use of the HIE.

2.3.2.3 Contains target audience strategies and measures.

2.3.2.4 Promotes an open process that is broadly inclusive of the health care community to be served and is not limited to entities that have a contractual relationship with a Participant in the QE.

2.3.3 Review of marketing and recruitment outcome measures against projected performance.

2.4 Ongoing monitoring and audits

In addition to QE’s obligations under or in accordance with the Oversight and Enforcement Policies, QEs shall ensure that an ongoing monitoring process includes:

2.4.1 Self-audits that track participation levels to ensure open community process. Activities will be reported through the QE governance process that tracks performance against measures established in the QE Marketing and Recruitment Plan.

2.4.2 That QEs shall ensure all stakeholder types across the community are represented and have a voice.
2.4.3 External audits and monitoring by the Certification Body will review marketing and recruitment outcome measures that track member participation.
3 Support for Adoption and Usage

Provide services to Participants that add value to participation and that include meaningful use support for HIE services (process and workflow); MPI maintenance (de-duplication of records and ability to link same person from other data sources).

3.1 Framework

The service should support:

3.1.1 Meaningful use of the HIE services to improve healthcare workflows
3.1.2 MPI maintenance
3.1.3 Interface connectivity to the HIE

3.2 QE Certification Evidence Requirements

QEs must be able to provide:

3.2.1 Copy of QE Adoption and Support Plan
3.2.2 Statistics that reflect use of Minimum Technical Requirements as outlined in the Qualified Entity (QE) Minimum Technical Requirements (as amended from time-to-time, the “Minimum Technical Requirements”)
3.2.3 An explanation of support services that:
   3.2.3.1 facilitate design and implementation
   3.2.3.2 explore available options, where feasible, in interface connectivity approaches
   3.2.3.3 highlight alternative mechanisms to support consent management
3.2.4 Examples of reports or other tools that are made available for better MPI management

3.3 Certification Tasks and QE Evaluation Standards

The Certification Body will be required to verify evidence provided by the QE including:

3.3.1 Existence of QE Adoption and Support Plan for time period.
3.3.2 Documentation of services offered that include at a minimum support for MU of the HIE, MPI maintenance and interface connectivity to the HIE.
3.3.3 Verification of the number of Participants using each service offered against actual vs. planned

3.4 Ongoing Monitoring and Audits

In addition to QE’s obligations under or in accordance with the Oversight and Enforcement Policies, QEs shall ensure that an ongoing monitoring process includes:

3.4.1 Self-audit that includes regular reporting and trending analysis of usage to the QE governance body (e.g., Board of Directors).
3.4.2 External audits by the Certification Body that evaluate a sampling, by practice, usage of services delivered against QE goal projections.
4. **Participant/Authorized User Training**

Provide a training and education program for all Authorized Users of the QE before allowing access to the system and annually or as needed based on any policy or procedure changes. Training will include but may not be limited to system integration, navigation, policies (privacy and security) and the appropriate use for role based access.

4.1 **Framework**

The service should:

4.1.1 Provide a training and education program for all Authorized Users:

4.1.1.1 Prior to allowing access to the HIE

4.1.1.2 At least annually or as needed based on any policy or procedure change

4.2 **QE Certification Evidence Requirements**

QEs must provide:

4.2.1 A QE Training and Education Plan/Curriculum

4.2.2 Logs of trainings completed that are maintained by Participants and made available upon request for audits

4.3 **Certification Tasks and QE Evaluation Standards**

The Certification Body will be required to verify evidence provided by the QE including:

4.3.1 Verification of the QE Training and Education Plan/Curriculum and training logs including annual logs.

4.3.2 Conformance based on QE logs including:

4.3.2.1 tracking logs for training(s) held for new Participants and/or Authorized Users that compare to new Participant Agreements

4.3.2.2 tracking logs for annual training(s) or as needed based on any policy or procedure change completed by Participants and/or Authorized Users that compare to full list or Participants and/or Authorized Users

4.4 **Ongoing Monitoring and Audits**

In addition to QE’s obligations under or in accordance with the Oversight and Enforcement Policies, QEs shall ensure that an ongoing monitoring process includes:

4.4.1 Self-audits that ensure that if training is delegated to Participants, the QE regularly collects attestation by Participants that specifies for which of their Authorized Users annual refresh training has occurred. If training is completed by QE, an attestation by QE that specifies for which of their Participants and/or Authorized Users annual refresh training has occurred.

4.4.2 External Audits by the Certification Body will assess that:

4.4.2.1 no one is authorized to use the system without the required training and that Authorized Users are routinely retrained

4.4.2.2 training on technology and policy compliance has occurred and will track and record the date of training and Authorized Users trained
5. User Support

Provide help desk and online service for Authorized User support to troubleshoot and resolve issues that may arise when accessing the system.

5.1 Framework

The service should:

5.1.1 Provide Authorized User support for technical issues that may arise when accessing the system that include:

   5.1.1.1 help desk support services
   5.1.1.2 online service support that provides a mechanism for submission of service requests

5.2 QE Certification Evidence Requirements

QEs must:

5.2.1 Provide a QE Authorized User Support Plan
5.2.2 Documentation of service requests received via help desk or online service for specified time period

5.3 Certification Tasks and QE Evaluation Standards

The Certification Body will be required to verify evidence provided by the QE including:

5.3.1 Verification of QE Authorized User Support Plan
5.3.2 Verification of help desk tracking logs for issues reported and issues resolved
5.3.3 Assessment of average time required to resolve issues against planned timeframes outlined in QE Authorized User Support Plan

5.4 Ongoing Monitoring and Audits

In addition to QE’s obligations under or in accordance with the Oversight and Enforcement Policies, QEs shall ensure that an ongoing monitoring process includes:

5.4.1 Self-audits that include:

   5.4.1.1 regular review of issue tickets and timeframe for resolution
   5.4.1.2 monthly reporting of volume and time to resolve
   5.4.1.3 percent within agreed timeframe as outlined in QE Authorized User Support Plan and outliers
   5.4.1.4 internal corrective action plans if performance is below standard

5.4.2 External audits and monitoring by Certification Body that:

   5.4.2.1 assess QE adherence to QE/QE Participant agreed upon resolution timeframes
   5.4.2.2 review “x” samples of help desk issue logs from submission to resolution with attention to percent that meet standard for resolution as noted in QE Authorized User Support Plan
6 Aligning with Stakeholder Priorities

Facilitate a collaborative process for Participants of the QE that is responsive to needs of Participants and priorities and that provides a feedback loop in order to support the identification and development of high value service solutions.

6.1 Framework

The process should:

6.1.1 Establish a mechanism for input from Participants and patients/consumers into development of service priorities, new services, enhanced functionality that builds value of health information exchange.

6.2 QE Certification Evidence Requirements

QEs must provide:

6.2.1 Evidence of stakeholder involvement that may include a description of the process for obtaining input from stakeholders.

6.3 Certification Tasks and QE Evaluation Standards

The Certification Body will be required to verify evidence provided by the QE including:

6.3.1 Verification that QE has a process for customer relations that:

6.3.1.1 is a clearly defined process for input on service priorities, solutions, added value initiatives.

6.4 Ongoing Monitoring and Audits

In addition to QE’s obligations under or in accordance with the Oversight and Enforcement Policies, QEs shall ensure that an ongoing monitoring process includes:

6.4.1 Validation that input to the business plan and enhancement of services is being sought and considered through self-evaluation of customer service approaches and outcomes.

6.4.2 External Audits and monitoring by Certification Body will assess the types and level of input by external stakeholders in the ongoing governance process.
Qualified Entity (QE) Organizational Characteristics Requirements

Version 1.2
REVISED June 2014

AS DEVELOPED THROUGH THE STATEWIDE HEALTH INFORMATION NETWORK OF NEW YORK (SHIN-NY) POLICY STANDARDS
Table of Contents

INTRODUCTION ..........................................................................................................................2
ORGANIZATIONAL CHARACTERISTICS ...........................................................................3
ORGANIZATIONAL INFORMATION .........................................................................................4
NON-PROFIT STATUS ..............................................................................................................5
GOOD STANDING IN NEW YORK STATE ..................................................................................6
GOVERNANCE STRUCTURE ......................................................................................................7
AVAILABILITY TO ALL PARTICIPANTS ....................................................................................8
COMPREHENSIVE, UP-TO-DATE LIST OF PARTICIPANTS .....................................................9
PARTICIPANT FLOW-DOWN REQUIREMENTS .......................................................................10
INSURANCE/LIABILITY COVERAGE .......................................................................................11
Introduction

This document outlines the requirements for Organizational Characteristics, and sets forth the minimum requirements for participation in the Statewide Health Information Network of NY (SHIN-NY) and certification as a Qualified Entity (the “Certification Requirements”). All capitalized terms used and not defined herein shall have the respective meanings given to such terms in the Privacy and Security Policies and Procedures for QEs and their Participants in New York State (as amended from time-to-time, the “Policies and Procedures”).

The Certification Requirements fall into the following four categories:

1. Organizational Characteristics, e.g., non-profit status, good standing in the State of New York, list of Participants, open board structure, necessary insurance. The Organizational Characteristics are outlined in this document.

2. Operational Requirements, e.g., infrastructure to operationalize the SHIN-NY requirements, including policies and practices for non-discriminatory exchange of data, system performance, member-facing services, business plans, audit procedures, participation in statewide policy development, and evaluation processes. These requirements are found in the Qualified Entity (QE) Member Facing Services Requirements (as amended from time-to-time, the “Member Facing Services Requirements”) as well as in sections of the Qualified Entity Participation Agreement (QEPA), as amended from time-to-time.

3. Policies and Procedures, e.g., approach for consent, authorization, authentication, access, patient engagement, audit, breach and sanctions. These requirements are found in the Policies and Procedures that outlines the policy implementation specifications.

4. Technical Services, e.g., baseline technical capabilities (i.e., Minimum Technical Requirements) and interoperability (i.e., SHIN-NY technical specifications) that users of the SHIN-NY can expect to be available within any region of the State of New York. These requirements are found in the Qualified Entity (QE) Minimum Technical Requirements (as amended from time-to-time, the “Minimum Technical Requirements”).

In order to participate in the SHIN-NY and become certified as a QE, pursuant to New York State regulations applicable to the SHIN-NY, an entity must satisfy the Certification Requirements. As such, the New York State Department of Health (NYS DOH) serves as the certification and monitoring entity to ensure the integrity of the SHIN-NY and maintain the public trust. NYS DOH, in its role as the certification and monitoring entity, can assign these functions to an outside entity that will be responsible for carrying out the certification process. “Certification Process” means the process by which an organization becomes qualified and re-certified as a Qualified Entity for participation in the SHIN-NY by demonstrating compliance with the Certification Requirements. “Certification Body” means NYS DOH or the entity designated by NYS DOH to oversee the Certification Process.

The NYS DOH may at its discretion, with input from the State Designated Entity Board of Directors, and based on an applicant’s ability to demonstrate its ability to fill gaps in services whether by geography or types of population, make a determination to waive certain organizational characteristics of a QE, so long as that QE adheres to the Operational Requirements, Policies and Procedures and Technical Services listed above.

QEs will actively participate in the Certification Process as described herein and participate in ongoing monitoring of their compliance with the Certification Requirements in accordance with the policies and procedures set forth in the Oversight & Enforcement Policies and Procedures for QEs (as amended from time-to-time, the “Oversight and Enforcement Policies”).

During the Certification Process, QE may propose an alternative method for satisfying a Certification Requirement or demonstrate that satisfaction of a Certification Requirement would impose an undue hardship on QE. The Certification Body, in its sole discretion, may elect to excuse such QE from satisfaction of such Certification Requirement.
Organizational Characteristics

In order to participate in the SHIN-NY and become certified as a QE, an entity must comply with the Certification Requirements, which are designed to protect and maintain the reliability, accuracy, and integrity of the SHIN-NY.

“Organizational Characteristics” are the set of Certification Requirements set forth herein relating to the following:

1. **Organizational Information:** (1) Address for all facilities; (2) Name and title of senior leadership

2. **Non-Profit Status:** Organized as a 501(c)3, whose incorporation articles have been filed with State of New York

3. **Good Standing in New York State:** Applicable certificates in New York State

4. **Governance Structure:** (1) Listing of Board members and their organizational affiliation on the candidate’s website; (2) Provision of organizational bylaws to the public upon request; (3) Public Health and physician representation on the Board, if possible; (4) Inclusive decision-making process; (5) transparency

5. **Availability to All Participants:** Provision of Minimum Technical Requirements (as such term is defined in the Minimum Technical Requirements) in accordance with the Minimum Technical Requirements and Member Facing Services (as such term is defined in the Member Facing Services Requirements) in accordance with the Member Facing Services Requirements

6. **Comprehensive, Up-to-Date List of Participants:** If QE has executed Participant Agreements with Participants, a list of such Participants and identification of such Participants that are providing data

7. **Participant Flow-Down Requirements:** If QE has executed Participant Agreements with Participants, procedures to address Participant compliance with the SHIN-NY Policy Standards

8. **Insurance/Liability Coverage:** Liability coverage relevant to the exchange of individually identifiable health information in accordance with such standards as may be required by regulation, SHIN-NY Policy Standards or the Qualified Entity Participation Agreement executed by the State Designated Entity and QE.
1. **Organizational Information**

To satisfy the Certification Requirements for Organizational Information, a QE shall publicly provide:

1.1 Address for all of its facilities.

1.2 Chief Executive Officer, Executive Director and other senior executives.

The QE shall supply the following evidence for purposes of certification:

1.3 Documentation of required organizational characteristics and attestation that the QE candidate will provide the Certification Body updated information as changes occur within 30 days of change.

The tasks to be performed by the Certification Body in the Certification Process include:

1.4 Verification of the QE candidate’s listing of facilities and leadership.

1.5 Verification of the QE candidate’s attestation to provide updated information as changes in the organization occur.

1.6 Performance of audits that confirms the QE Organization Information meets the Certification Requirements.

1.7 Acceptance and recording of all changes as submitted by QE to the Certification Body related to Organization Information.

1.8 **Standard for QE to meet Certification Requirements**: Documentation contains all required information.

In addition to QE’s obligations under or in accordance with the Oversight and Monitoring Policies, QEs shall ensure that an ongoing monitoring process includes:

1.9 Self-audits that will identify any organizational changes.

1.10 Reporting any changes to the Certification Body as required within 30 days.
2. **Non-Profit Status**

To satisfy the Certification Requirements for Non-Profit Status, a QE shall:

2.1 Be a non-profit organization incorporated in New York State with federal tax-exempt status.

The QE shall supply the following evidence for purposes of certification:

2.2 New York Certificate of incorporation pursuant to Section 402 of the Not-for-Profit Corporation Law.

The tasks to be performed by the Certification Body in the Certification Process include:

2.3 Verification of the QE candidate’s New York Certificate of Incorporation.

2.4 Notation of reports from the QE of any change in non-profit status.

2.5 Confirmation of QE non-profit status as part of its audit process.

2.6 **Standard for QE to meet Certification Requirements:** Documentation meets New York State incorporation requirements.

In addition to QE’s obligations under or in accordance with the Oversight and Monitoring Policies, QEs shall ensure that an ongoing monitoring process includes:

2.7 Self-audits that will identify any non-profit status changes.

2.8 Reporting mechanism for all changes as required to the Certification Body.
3. **Good Standing in New York State**

To satisfy the Certification Requirements for Good Standing in New York State, a QE shall:

3.1 Have in place the New York Charities Registration from the Attorney General.

3.2 Have in place the New York Vendor Responsibility Registration from the Office of the State Comptroller.

The QE shall supply the following evidence for purposes of certification:

3.3 Evidence of all applicable New York State certificates.

The tasks to be performed by the Certification Body in the Certification Process include:

3.4 Verification of all applicable New York State certificates supplied by the QE.

3.5 Notation and recording of all reports from the QE related to any changes in standing in New York State.

3.6 Certification Body’s audit confirms and validates QE’s status in Good Standing in New York State.

3.7 **Standard for QE to meet Certification Requirements**: QE documentation related to New York State registrations meets New York State standards and is up to date.

In addition to QE’s obligations under or in accordance with the Oversight and Monitoring Policies, QEs shall ensure that an ongoing monitoring process includes:

3.8 Self-audits that regularly review QE’s New York State registrations to ensure they are up to date.

3.9 Notification to Certification Body of change of status related to New York State required non-profit registrations within 30 days.
4. Governance Structure

To satisfy the Certification Requirements for Governance Structure, the QE shall:

4.1 Maintain an up to date list of Board members and their organizational affiliation on the QE candidate’s website.

4.2 Make the organization bylaws available to the public upon request.

4.3 If possible, include Public Health and physician representation on the Board.

4.4 Provide an inclusive decision-making process characterized by multi-stakeholder participation that includes stakeholder representatives that reflect the QE service area. Examples of such stakeholder representatives may include but are not limited to: (a) physician groups, (b) sole practitioners and small ambulatory physician offices (i.e., between 1-5 physicians), (c) diagnostic and treatment centers and licensed clinicians providing mental health and substance abuse services, (d) community health centers or federally qualified health centers (FQHCs), (e) a county or municipal Public Health Department, (f) general hospitals, (g) long-term care providers, including long-term Home Health Care providers, (h) data suppliers, including pharmacies, laboratories and imaging centers, (i) insurers and purchasers (e.g., employers), (j) rural health networks and (k) New Yorkers as patient/consumer representatives.

4.5 Provide regular opportunities for public attendance, comments and feedback at meetings of its board of directors, and publish minutes of meetings

The QE shall supply the following evidence for purposes of certification:

4.6 Up to date list of Board members with evidence of its presence on the QE website. Documentation of QE Bylaws with evidence that supports availability to the public upon request.

4.7 Documentation substantiating the multi-stakeholder inclusivity requirements.

The tasks to be performed by the Certification Body in the Certification Process include:

4.8 Review and verification that the QE candidate’s description of its governance structure, website, and availability of bylaws to the public meet the Governance Structure requirements in 4.1, 4.2, 4.3, and 4.4.

4.9 Notation and recording of and changes and or non-conformance to the QE governance structure as reported by the QE.

4.10 Confirmation of QE conformance with governance structure requirements as part of its audit process.

4.11 **Standard for QE to meet Certification Requirements**: QE governance structure documentation and website postings meets the Certification Requirements for governance structure.

In addition to QE’s obligations under or in accordance with the Oversight and Monitoring Policies, QEs shall ensure that an ongoing monitoring process includes:

4.12 Self-audits that monitor and report changes in governance structure or participation.
5. Availability to All Participants

To satisfy the Certification Requirements for Availability for All Participants, the QE shall:

5.1 Provide the minimum technical requirements in accordance with the minimum technical requirements and the Member Facing Services in accordance with the Member Facing Service Requirements to Participants who enter into a Participant Agreement with QE. The QE must enter into Participation Agreements with all willing Practitioners, Provider Organizations, health homes and Payers (as such terms are defined in the Policies and Procedures) within the geographic or functional service area of the QE that commit to meet the QE’s reasonable terms for participation, and specifically cannot make a pre-requisite for participation that the Participant have a contractual relationship with any other Participant in the QE. Allied Individuals and Organizations will have limited agreements with QEs for receipt of alerts.

The QE shall supply the following evidence for purposes of certification:

5.2 Attestation through the signed QEPA that the QE will provide the Minimum Technical Requirements and Member Facing Services to Participants who enter into a Participant Agreement with QE.

The tasks to be performed by the Certification Body in the Certification Process include:

5.3 Verification of the signed QEPA by the QE candidate.

5.4 Verification of the signed Participant Agreement between the QE and the Participant.

5.5 Notation and recording of any rejections of Participants as reported to the Certification Body by the QE.

5.6 Audit that monitors policies and procedures of a random selection as determined by the Certification Body of applicable Participants.

5.7 Event audits that are triggered by rejection complaints.

5.8 **Standard for QE to meet Certification Requirements**: Attestation through the QEPA that commits the QE to providing Minimum Technical Requirements and Member Facing Services to Participants who enter into a Participant Agreement with QE.

In addition to QE’s obligations under or in accordance with the Oversight and Monitoring Policies, QEs shall ensure that an ongoing monitoring process includes:

5.9 Self-audits that track and report changes in policy related to participation in QE’s network by Participants to the Certification Body.

5.10 Process for justification and reporting of participation rejections to Certification Body.
6. **Comprehensive, Up-to-Date List of Participants**

To satisfy the Certification Requirements for managing the Comprehensive, Up-to-Date List of Participants, the QE shall:

6.1 Comprise a list of all Participants and identify such Participants that are providing data as required in the Policies and Procedures.

6.2 At a minimum, update the list quarterly.

6.3 Publish the list on the QE’s website.

The QE shall supply the following evidence for purposes of certification:

6.4 Evidence of the process for comprising and maintaining updated lists of Participants.

6.5 Website screenshots that evidence the existence of the complete list on the site.

6.6 Evidence that the list includes designations for those Participants that are supplying data.

The tasks to be performed by the Certification Body in the Certification Process include:

6.7 Review and verification that a significant sample of Participants as supplied by the QE candidate is complete, up to date, and indicates those Participants that supply data.

6.8 Notations and recording of any changes to the list of Participants as reported by the QE.

6.9 Confirmation during the audit that the contact information corresponding to the list of Participants is accurate, up to date, and is posted on the QE website.

6.10 **Standard for QE to meet Certification Requirements**: The list of Participants contains the accurate legal or trade name of the Participant and a designation as to whether or not they are supplying data.

In addition to QE’s obligations under or in accordance with the Oversight and Monitoring Policies, QEs shall ensure that an ongoing monitoring process includes:

6.11 Self-audits that ensure tracking and correction of the list of Participants as changes occur.

6.12 Notification related to changes to the list of Participants through website posting of corrected and/or updated list.
7. Participant Flow-Down Requirements

To satisfy the Certification Requirements for managing Participant Flow-Down Requirements, the QE shall:

7.1 Establish monitoring and enforcement policies and procedures for compliance by Participants, with all applicable SHIN-NY Policy Standards.

7.2 Inform all Participants about the monitoring and enforcement policies.

The QE shall supply the following evidence for purposes of certification:

7.3 Copy of the QE monitoring and enforcement policies and procedures.

7.4 Copy of the Participant Agreement between the QE and the Participant that includes the flow-down requirements for adhering to the SHIN-NY Policy Standards as set forth in the SHIN-NY Policy Standards.

The tasks to be performed by the Certification Body in the Certification Process include:

7.5 Review and verification that the Participant Agreements between the QE and the Participant contain flow-down requirements for adhering to the SHIN-NY Policy Standards as set forth in the SHIN-NY Policy Standards.

7.6 Review of QE monitoring and enforcement policies.

7.7 Verification of QE’s notification regarding the QE monitoring and enforcement policies to all Participants.

7.8 Review and confirmation that the Participant Agreements between the QE and the Participant contain all of the flow-down requirements for adhering to the SHIN-NY Policy Standards as set forth in the SHIN-NY Policy Standards during the audit process.

7.9 Standard for QE to meet Certification Requirements:

7.9.1 QE has monitoring and enforcement policies to promote compliance by Participants with SHIN-NY Policy Standards.

7.9.2 QE contractual arrangements meets requirements for Participant Agreements set forth in applicable law, the SHIN-NY Policy Standards and the QEPA.

7.9.3 Agreements contain flow-down requirements for adhering to SHIN-NY Policy Standards as set forth in the SHIN-NY Policy Standards.

In addition to QE’s obligations under or in accordance with the Oversight and Monitoring Policies, QEs shall ensure that an ongoing monitoring process includes:

7.10 Self-audits that identify gaps in application of monitoring and enforcement policies and procedures.

7.11 Notification to the Certification Body of changes in QE monitoring and enforcement policies and procedures that impact the flow-down requirements for Participants within 30 days.
8. Insurance/Liability Coverage

To satisfy the Certification Requirements for Insurance/Liability Coverage, the QE shall:

8.1 Secure insurance liability coverage as outlined and agreed to in the QEPA so as to reduce the risk of exposure as a result of the exchange of individually identifiable health information.

The QE shall supply the following evidence for purposes of certification:

8.2 Copy of the QE’s certificate of insurance and other relevant supporting documentation, including copies of insurance policies, if appropriate.

The tasks to be performed by the Certification Body in the Certification Process include:

8.3 Review of and verification that the QE’s certificate of insurance and other relevant supporting documentation meets the requirements as outlined in the signed QEPA.

8.4 Notation and recording of any changes to the levels of insurance coverage as reported by the QE.

8.5 Confirmation of validity of QE’s certificate of insurance and other relevant supporting documentation as part of the review process.

8.6 **Standard for QE to meet Certification Requirements:** QE documentation of insurance coverage meets the agreed upon levels as outlined in the QEPA.

In addition to QE’s obligations under or in accordance with the Oversight and Monitoring Policies, QEs shall ensure that an ongoing monitoring process includes:

8.7 Self-audits that ensure the appropriate coverage level is maintained.

8.8 Notification of any QE insurance coverage levels to the Certification Body.