Oversight & Enforcement
Policies and Procedures for QEs

Version 1.2

REVISED June 2014

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

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

referenced in the Non-Compliance Complaint, nature and existence of any past or pending investigations with respect to the Non-Compliance Complaint.

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).