

# Oversight & Enforcement Policies and Procedures for QEs

Version 1.6

**REVISED January 2024**

**AS DEVELOPED THROUGH THE NEW YORK  
STATEWIDE COLLABORATION PROCESS (SCP)**

# Table of Contents

<b>Introduction</b> .....	3
<b>Definitions</b> .....	4
<b>1. Oversight</b> .....	5
1.1 Complaints Process .....	5
1.2 Internal Investigation and Reporting.....	5
1.3 External Investigation and Reporting Process.....	6
1.4 Audits .....	7
1.5 Record Retention.....	7
<b>2. Enforcement</b> .....	8
2.1 Types of Enforcement Actions .....	8
2.2 Determining Applicable Enforcement Action .....	8
2.3 Application of Enforcement Actions.....	8
2.4 Grievance .....	9
2.5 Documentation.....	9

## Introduction

The New York State Department of Health (NYS DOH) is responsible for the oversight and enforcement of the SHIN-NY Regulation and related SHIN-NY Policy Guidance. The purpose of this document is to provide a high-level description of the procedures by which the NYS DOH, or its designee, will perform basic oversight of Qualified Entities (QEs). This includes requirements and enforcement actions for QE self-audits, complaints, external monitoring, audits, and investigations.

Authority for Oversight, Monitoring and Enforcement of QEs is outlined in Section 300.2 of the SHIN-NY Regulation § Part 300, Establishing the SHIN-NY, and is cited below.

The New York State Department of Health shall:

- (a) Oversee the implementation and ongoing operation of the SHIN-NY.
- (b) Implement the infrastructure and services to support the private and secure exchange of health information among qualified entities and qualified entity participants.
- (c) Administer the statewide collaboration process and facilitate the development, regular review and update of SHIN-NY policy guidance.
- (d) Perform regular audits, either directly or through contract, of qualified entity functions and activities as necessary to ensure the quality, security and confidentiality of data in the SHIN-NY.
- (e) Provide technical services, either directly or through contract, to ensure the quality, security and confidentiality of data in the SHIN-NY.
- (f) Assess qualified entity participation in the SHIN-NY and, if necessary, suspend a qualified entity's access to or use of the SHIN-NY, when it reasonably determines that the qualified entity has created, or is likely to create, an immediate threat of irreparable harm to the SHIN-NY, to any person accessing or using the SHIN-NY, or to any person whose information is accessed or transmitted through the SHIN-NY.
- (g) Publish reports on health care provider participation and usage, system performance, data quality, the qualified entity certification process, and SHIN-NY security.
- (h) Take such other actions as may be needed to promote development of the SHIN-NY.

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 *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 (QEPA).

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. Any additional investigations and audits would follow the procedures described in the external audit and/or investigation section of the policies and procedures described herein.

For a QE to participate in the SHIN-NY, they must comply with applicable state, federal and local law as well as the Certification Requirements. The Certification Requirements are designed to protect and maintain the reliability, accuracy, and integrity of the SHIN-NY. The four categories of Certification Requirements (Organizational Characteristics, Operational Requirements, Policies and Procedures, and Technical Services) are described in the *Qualified Entity (QE) Organizational Characteristics Requirements*, as amended periodically.

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 resolve non-compliance.

Together with the Certification Process, implementation of the Oversight and Enforcement Policies 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 periodically (the "Policies and Procedures").

**Certification Body** is the NYS DOH or a third-party entity designated by NYS DOH to conduct QE Certification and ongoing monitoring assessment activities that are coordinated and managed by the State Designated Entity (SDE).

**Certification Process** is defined in the *Qualified Entity (QE) Certification Process* as amended from time-to-time.

**Certification Requirements** is defined in the *Qualified Entity (QE) Organizational Characteristics Requirements, QE Participant Member Facing Services Requirements, Minimum Core Services Technical Requirements, and the SHIN-NY Privacy and Security Policies and Procedures for QEs and their Participants* as amended from periodically.

**Enforcement Actions** means particular sanctions and/or corrective action plans that may be imposed by the Oversight Entity on a QE found to be out of compliance with federal, state, or local law and the SHIN-NY Regulation and Certification requirements and are based on the nature and severity of the non-compliance as determined by the Oversight Entity.

**Grievance Process** is outlined in the *QE Certification Process and Procedures*. The Oversight Entity will review any grievances and make a determination according to the evidence submitted by the QE as well as the original findings for the non-compliance determination.

**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.

**Oversight Entity** is the NYS DOH. Periodic monitoring of QEs shall be the responsibility of NYS DOH or a third-party designated by NYS DOH.

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

# 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 and describes the mechanisms for investigating potential non-compliance. All Non-Compliance, regardless of the method of detection, will be addressed by the Oversight Entity who will gather the information necessary for determining what, if any, corrective actions are appropriate.

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;
- (c) an external audit and internal 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;

The following outlines the policies and procedures for (i) The Complaints Process, (ii) Internal Investigation and Reporting, (iii) External Investigation and Reporting, (iv) Audits, and (v) Record Retention.

## 1.1 Complaints Process

- 1.1.1 Each QE shall develop and implement policies and procedures for receiving, investigating and responding to complaints from stakeholders of the SHIN-NY, including Participants. Such policies should include both non-compliance complaints as well as general complaints.
- 1.1.2 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.
- 1.1.3 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.
- 1.1.4 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 1.2: Internal Investigations and Reporting of these procedures. If a Non-Compliance Complaint is filed with the Oversight Entity, the Oversight Entity shall follow the procedures set forth in either Section 1.2: Internal Investigations and Reporting or Section 1.3: External Investigation and Reporting outlined in these procedures.

## 1.2 Internal Investigation and Reporting.

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

- 1.2.3 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. Following an Internal Investigation conducted pursuant to Section 1.2.1 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, the SHIN-NY enterprise, and/or any Participants that may have been harmed resulting from the Non-Compliance.
- 1.2.4 If the Oversight Entity directs the QE to perform an Internal Investigation based on a suspected non-compliance issue reported to the Oversight Entity, the QE shall report the results of such investigation to the Oversight Entity upon completion of the internal investigation. If the QE did not detect Non-Compliance as a result of such Internal Investigation, QE shall provide to the Oversight Entity a written statement that no Non-Compliance was detected, and a summary of the Internal Investigation conducted outlining the investigation findings.

### **1.3 External Investigation and Reporting Process**

- 1.3.1 Upon receipt of a Non-Compliance Complaint by the Oversight Entity, the Oversight Entity will 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 1.2.1: Internal Investigations and Reporting and provide any reports or notices required by that Section.
- 1.3.2 If the Oversight Entity determines that it will conduct an External Investigation, the Oversight Entity will begin the External Investigation within 30 days after receipt of a Non-Compliance Report or a Non-Compliance Complaint. To begin the External Investigation, the Oversight Entity will 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”) will include a summary of the intended External Investigation, including any requests for additional information from the QE, the Participant and/or the complainant.
- 1.3.3 Each QE will require 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.
- 1.3.4 The Oversight Entity will document its findings (“Report of Findings”) in response to the receipt of a Non-Compliance Complaint. If the investigation is conducted on behalf of the Oversight Entity by a third-party assessor, a Report of Findings will be submitted to the Oversight Entity upon completion of the investigation. In either case the Report of Findings will be shared with the applicable QE. Such Report of Findings will 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 and recommendations for corrective action if required.
- 1.3.5 The Oversight Entity will finalize the Report of Findings as soon as reasonably practicable after the receipt of a Non-Compliance Report or a Non-Compliance Complaint.

**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, or history of complaints similar to the Non-Compliance Complaint with respect to the applicable QE(s).

## 1.4 Audits

### 1.4.1 External Audits at the Discretion of the Oversight Entity

- 1.4.1.1 The Oversight Entity may, in conjunction with its ongoing monitoring, conduct periodic assessments of specific state, federal and local law and Certification Requirements. In circumstances where the audit assessment is performed by a third-party designee of the Oversight Entity, the third-party will submit a report of findings and recommendations for potential follow up actions to the Oversight Entity.
- 1.4.1.2 Typically, external Audits will be performed during regular business hours upon reasonable notice to the QE. However, the Oversight Entity may at its discretion perform an audit with no advance notice to the QE. 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.
- 1.4.1.3 The QE shall require its Participants to cooperate with the Oversight Entity in connection with any External Audit, including by providing the Oversight Entity access to records, and other sources of information related to the scope of the External Audit.
- 1.4.1.4 The results of any External Audit will be documented in a written report (External Audit Report) by the Oversight Entity or its designee and shared with the applicable QE. Such External Audit Report will 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 (d) a root cause analysis if non-compliance occurred (e) and recommendations for corrective action if required.
- 1.4.1.5 The Oversight Entity will finalize the External Audit Report as soon as reasonably practicable after providing notice to the QE of its intention to perform an External Audit.

### 1.4.2 QE Audits, Self-Monitoring and Reporting.

- 1.4.2.1 Each QE shall perform 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 as part of the QE Certification Process.
- 1.4.2.2 As stated in the Privacy & Security Policies and Procedures Section 6: Audit: Sub-section 6.2 a 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 applicable state, federal and local law and the Certification Requirements. QEs shall have policies and procedures in place for this monitoring process to be checked as part of the QE Certification Process.

## 1.5 Record Retention

- 1.5.1 Each QE shall retain records relating to this Section (including the results of all Self-Audits and all Non-Compliance Reports) for a period of at least six (6) years.
- 1.5.2 The Oversight Entity will retain records relating to this Section (including all Investigation Notices, Reports of Findings, External Audit Reports, Non-Compliance Reports, Non-Compliance Complaints) for a period of at least six (6) years.

## **2. Enforcement**

The NYS DOH as the Oversight Entity has authority to impose Enforcement Actions that may include particular sanctions and/or corrective action plans on a QE or QEs who have been found to be out of compliance with federal, state, and local law or the SHIN-NY Regulation and Certification Requirements. The Enforcement Actions imposed on a QE will be based on the nature and severity of Non-Compliance as determined by the Oversight Entity.

### **2.1 Types of Enforcement Actions**

- 2.1.1 Enforcement Action Resolutions imposed by the Oversight Entity may 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 resolve 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, or
  - (f) imposition of withholding of State funding allocations 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 will consider the following factors in determining the appropriate Enforcement Action to be applied:
- (a) Nature and extent of Non-Compliance and the extent of actual or potential harm to any stakeholder in the SHIN-NY and/or the SHIN-NY enterprise resulting from Non-Compliance.
  - (b) QE's level of responsibility i.e., was the nature of the circumstances leading to or causing Non-Compliance inadvertent, negligent, reckless, or intentional.
  - (c) 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.
  - (d) QE's history of prior compliance.
  - (e) Consideration of the possible impact the Resolution may have on the QE Participants.
  - (f) Such other factors as the Oversight Entity may deem appropriate.

### **2.3 Application of Enforcement Actions**

- 2.3.1 Upon review of the Report of Findings or External Audit Report, as applicable, the Oversight Entity will determine the applicable Enforcement Action to be imposed on the QE in accordance with the guidelines set forth in this Section 2.2.
- 2.3.2 The Oversight Entity will maintain documentation of the process that was used for determining the applicable Enforcement Action including documentation of all factors considered.
- 2.3.3 The Oversight Entity will provide written notice of the Enforcement Action to the QE that will include (a) reference to the applicable Report of Findings or External Audit Report, (b) the Resolution (c) any applicable timeframes, (d) the factors considered when determining the Resolution and (e) the process for submitting a grievance to the determination.



## **2.4 Grievance**

- 2.4.1 The QE has the right to submit a grievance in writing the Oversight Entity's imposition of a non-compliance Enforcement Action and Resolution no later than 60 days after receipt by the QE of notification of such Enforcement Action. The grievance will follow the QE Certification grievance process as outlined in the QE Certification Process and Procedures guidance document.
- 2.4.2 The Oversight Entity will inform the QE in writing of its decision regarding the imposed Enforcement Action.

## **2.5 Documentation**

- 2.5.1 The Oversight Entity will retain records relating to this Section (including all Enforcement Action Notices and all documentation relating to determination of Enforcement Resolutions for at least six (6) years after a final determination is made with respect to each Resolution.