Qualified Entity (QE) Minimum Core Services Technical Requirements

Version 1.6

REVISED January 2023

AS DEVELOPED THROUGH THE STATEWIDE Collaboration Process (SCP)

Table of Contents

Introduction

This document sets forth the minimum core services technical requirements that organizations must fulfill to be considered New York State Qualified Entities (QEs). The requirements are evaluated as part of the QE Certification Process by the NYS DOH designated third-party Certification Body that is under contract with the State Designated Entity. 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 Core Services are the essential services described herein that each Qualified Entity must provide in an acceptably common format, as certified by the Certification Body.

Local QE Components and Requirements means any minimum technical requirement that must be enabled to serve, at minimum, local QE participants.

Statewide SHIN-NY Components and Requirements means any minimum technical requirement that must be enabled, at minimum, statewide. Potential opportunities for future Statewide SHIN-NY technical innovations are noted where applicable.

Minimum Core Services Technical Requirements

Qualified Entities are certified based on their ability to deliver or enable the delivery of the essential core services described in this document. Minimum technical requirements are distinguished by how they are 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 the SHIN-NY. All Qualified Entities have an executed Qualified Entity Participation Agreement (QEPA) with the State Designated Entity that sets forth the roles and responsibilities of both entities and establishes the QE requirements for enabling health information exchange via the SHIN-NY on behalf of their Participants.

The following table summarizes the minimum core services requirements and identifies distinctions between those services that are local and/or cross-community (statewide) in nature.

Service	Local QE Components and Requirements	Statewide SHIN NY Components and Requirements
Patient Record Lookup	• Local MPI • Clinical Viewer • Interface with 3rd Party Software (incl. EMR/EHR)	• Access to data across QE systems • Utilize statewide services (e.g., Enterprise Hub and sMPI)
Secure Messaging	• Provider Directory / Master Clinician Index • Clinical Viewer – Provider Portal • Interface to 3rd Party Software • Secure Messaging or Direct Message Protocols	N/A

Service	Local QE Components and Requirements	Statewide SHIN NY Components and Requirements
Consent Management	• Support service and / or online tool provided by QE • Interface with 3rd Party Software • Local implementation details left to QE • Subject to statewide policy	• Centralized Consent Hub manages patient "All-In Consent" (AIC) status and notifies QEs when AIC is granted or modified • Facility-based consent is evaluated by initiating QE to allow access to patient records across the state • "Break the glass" events reported cross- community as part of Patient Record Lookup service • Subject to statewide policy
Notifications (Alerts)	• Support service and / or online tool provided by QE • Local QE follows its standard local processes to accept a subscription from the user	• QEs communicate cross-community notifications to other QEs (for border providers, patients traveling for treatment, etc.) • Receiving QE uses alerts appropriately based on treatment relationship, subscription, and consent
Identity Management & Security	• Self-service and administrative help desk support • Two-factor authentication (as required)	• Future opportunity for centralized user authentication
Provider and Public Health Clinical Viewer	• Clinical viewer must be accessible and available to providers and public health agencies • Local implementation details and features left to QE	• Future opportunity for centralized clinical viewer for public health
Results Delivery	• Presentation in Clinical Viewer • Interface with 3rd Party Software at QE's discretion • Secure Email/Direct Message Protocol • Based on local demands for service • Lab and radiology at minimum • Delivery to ordering provider, at a minimum	• N/A
Public Health Integration	• Local implementation details and features left to QE • Based on agreements with local public health agencies	• Future opportunity for centralized public health use-cases
Potential New Statewide Core Service		
Clinical Data Exchange Between QEs and Between QEs and Public Health Departments	• N/A	• Centralized services to support initiatives to exchange clinical data between QEs and between QEs and Public Health Departments • Future opportunity for analytics, reporting use • Includes discrete data (based on implementation of FHIR framework)

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 across a broader nationwide network when available and connected to the SHIN-NY. This service enables the matching of patient records at a local level using patient specific demographic information or local facility medical record numbers (MRNs). A local master patient index (MPI) is 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 (sMPI). This service provides 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 perform the following:

1.1.1 Patient-Selection Query: 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 and medical record number (or equivalent, [i.e., member number]) pair

1.1.2 Document-List Query: 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

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,

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),

1.1.3 Search Origination – QE: Search from within a QE's clinical viewer

1.1.4 Search Origination – Third Party Software: Search from within third party software, including query and retrieve from Certified Applications (as defined in the SHIN-NY Policies and Procedures) such as EMR/EHR system, 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 support of a query from the third party software, and testing and supporting the query interface is economically feasible and sustainable for the QE; third party software interfaces are supported at the QE's discretion

1.1.5 Document-Retrieval Query: After selecting a patient, retrieve records from all desired data sources known to the local QE

1.1.6 Emergency Break the Glass: Indicate that a patient lookup request is a request to "break the glass" due to an emergency condition as defined in Section 1.2.4 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 Certification Requirements

To enable user requirements, QEs must:

1.2.1 Provide query ability to Authorized Users as described in § 1.1

1.2.2 Receive and respond to queries from the SHIN-NY for a specific MPI and return a CCDA or other information to the SHIN-NY, as defined in the Statewide PRL: Statewide MPI (sMPI) and PRL (sPRL) Functional Specification.

1.2.3 Notify querying QE that no match was found. Querying QE may display, log, or dismiss such "no match" responses

1.2.4 Make CCDA or other information available via clinical viewer, third party software or patient portal to all validated Authorized Users connected to a QE

1.2.5 Conform to standards and specifications established in the Statewide PRL (sPRL) functional specifications.

1.2.6 Support SHIN-NY access control specifications and identity management requirements established pursuant to the *SHIN-NY Privacy & Security Policies and Procedures for QEs and their Participants*

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 or that a consent exception exists 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.

1.2.7.3 Provide an exception to ordinary consent restrictions that are outlined in the Privacy and Security Policies and Procedures for QEs and their Participants as appropriate.

1.2.8 Log all patient record lookup requests sent and received, as well as audit data specified by the SHIN-NY Policies and Procedures

1.2.8.1 Separately audit all requests to "break the glass" on patient consent restrictions in the case of an emergency condition

1.3 QE Service Level Requirements for Certification

Conformance to service levels for reliability and availability of user requirements as outlined in Service Level Agreements (SLAs) between a QE and their Participants.

2. Secure Messaging

Secure messaging services provide Authorized Users with the ability to send peer-to-peer messages between two trusted providers. The Secure Messaging Solutions are HIPAA compliant and protect data both at rest and in transit. They also encrypt data and incorporate authentication controls, integrity controls, and maintain an audit trail satisfying all HIPAA requirements. A QE HIPAA secure messaging platform should have these characteristics:

- Secure Encryption: Security measures should enable the safe transmission of electronic protected health information (ePHI) following industry-standard protocols and each message should be secured with a unique encryption key to ensure that patients' data remains private
- Centralized Storage: HIPAA requirements outline the need for a secure storage center for messages. Secure cloud-based storage facilitates comply with data retention policies by providing centralized storage management capabilities
- Message Delivery Notifications: Secure messaging approaches should provide notifications of successful message delivery, confirming the message was delivered to the intended recipient
- Account Management and Controls: QE account administrators should have the ability to record and monitor all transmissions containing ePHI as part of the QE auditing process

2.1 User Requirements

Through secure messaging 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 Authorized Users

2.1.3 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 PRL: Statewide MPI (sMPI) and PRL (sPRL) Functional Specification

2.1.3.1 Responding QE must be able to determine that the address provided is valid and securely associated with the requesting provider

2.1.4 Receive and decrypt messages to the provider from any secure communication source

2.2 QE Certification Requirements

To enable secure messaging, QEs 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 industry-wide secure messaging standards and specifications

2.2.3 Have messages encrypted in transport according to standards defined by U.S. Health and Human Services Department Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

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 Log all messages sent and received, as well as audit data specified, as required by the SHIN-NY Policies & Procedures

2.2.7 Have established secure messaging service levels for reliability and availability

2.3 QE Service Level Requirements for Certification

Conformance to service levels for reliability and availability of user requirements as outlined in Service Level Agreements (SLAs) between a QE and their Participants.

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 SHIN-NY 10 NYCRR Part 300 and the Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 NYCRR § 300.3(b)(1).

New York and SHIN-NY patient record consent policy is defined as “consent to access”. Access must be explicitly granted in writing to providers by patients “opting in” to data access. Written consent can be collected by individual provider organizations and communicated to one or more QEs, or a patient can sign an “All-In Consent” form (when available) that grants consent to all their current and future treating providers and health plans. QEs maintain registry of patient consent decisions for individual- and multi-provider organizations and “All-In Consent”. The QE consent registry, and all relevant consents, must 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 these secure messages. The Authorized User is responsible for ensuring 1:1 exchange messages are appropriate under implied or written consent as required by law and the SHIN-NY Policies and Procedures.

3.1 User Requirements

Through Consent Management 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 (i.e., “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
- 3.1.5.2 QE Authorized Users request testing and support of a consent management interface from the third party software, and testing and supporting the query interface is economically feasible and sustainable for the QE; 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 situations as defined by SHIN-NY Policies and Procedures

- 3.1.7.1 Gain access by Public Health Users without patient affirmative consent for applicable Public Health uses as defined in SHN-NY Policies and Procedures and State, local, and city law.

3.2 QE Certification Requirements

To enable consent management, QEs 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 Maintain a connection to the SHIN-NY's Centralized Consent Hub when available, in order to send and receive All-In Consent status updates for patients who grant All-In Consent or change their All-In Consent status

3.2.2.1 Maintain accurate All-In Consent status for patients in the QE repository and include All-In Consent status during all consent checks for access to data

3.2.2.2 Conduct regular audits of data access based on All-In Consent, to ensure access is for allowable purposes, as defined by SHIN-NY Policies and Procedures and New York State Law

3.2.3 Conform to all standards regarding consent management as defined by SHIN-NY Policies and Procedures and New York State Law

3.2.4 Adequately log and communicate "break the glass" events in patient record lookup requests, via notification messages or through other methods as defined by SHIN-NY Policies and Procedures. Provide a method for an Authorized User to verify the consent status of a patient

3.3 QE Service Level Requirements for Certification

Conformance to service levels for reliability and availability of user requirements as outlined in Service Level Agreements (SLAs) between a QE and their Participants.

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 PRL: Statewide MPI (sMPI) and PRL (sPRL) Functional Specification and the SHIN-NY Privacy and Security Policies and Procedures for QEs and their Participants.

4.1 User Requirements

Through notification/alerts services available from the QE, an Authorized User—through either direct subscription management capabilities or via change request submitted to a QE helpdesk—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
- 4.1.1.4 Patient transfer

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 Certification Requirements

To enable notifications (alerts), QEs 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, discharges, and transfers

- 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 Statewide PRL: Statewide MPI (sMPI) and PRL (sPRL) Functional Specification

4.2.3 Deliver notifications to subscribers when data required to detect a notifiable event is transmitted to the QE by a data provider and in accordance with all consent requirements of the SHIN-NY Policies and Procedures

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 SHIN-NY Policies and Procedures

4.2.7 Conform to standards and specifications established by the Statewide PRL: Statewide MPI (sMPI) and PRL (sPRL) Functional Specification

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

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

4.3 QE Service Level Requirements for Certification

Conformance to service levels for reliability and availability of user requirements as outlined in Service Level Agreements (SLAs) between a QE and their Participants.

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 via the SHIN-NY.

5.1 User Requirements

Through Identity Management and Security 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 as outlined in the Participant Member Facing Services policy guidance document.

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 Certification Requirements

To enable identity management and security, QEs must:

5.2.1 Support multiple roles with configurable levels of access to SHIN-NY data, including access to limited data sets by role as developed 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 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 PRL: Statewide MPI (sMPI) and PRL (sPRL) Functional Specification and the SHIN-NY Policies and Procedures.

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, inappropriate access, 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 PRL:

Statewide MPI (sMPI) and PRL (sPRL) Functional Specification

5.2.11 Immediately notifying and escalating known or suspected breaches of security according to the SHIN-NY Policies and Procedures.

5.3 QE Service Level Requirements for Certification

Conformance to service levels for reliability and availability of user requirements as outlined in Service Level Agreements (SLAs) between a QE and their Participants.

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 via a clinical viewer platform.

6.1 User Requirements

Through the clinical viewer 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 the 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 and the Centralized Consent Hub, 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., eHealth Exchange, Veterans Administration, etc.) with which the QE may also contract

6.2 QE Certification Requirements

To enable provider and public health clinical viewer, QEs must:

6.2.1 Control access using role-based access control as per the SHIN-NY Policies and Procedures Section 2: Authorization

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 SHIN-NY Policies and Procedures

6.3 QE Service Level Requirements for Certification

Conformance to service levels for reliability and availability of user requirements as outlined in Service Level Agreements (SLAs) between a QE and their Participants.

7. Results Delivery

Delivery of diagnostic results and reports back to ordering providers and others designated to receive results. This service is based on local and regional demand.

7.1 User Requirements

Through the results delivery services available from the QE, an Authorized User must be able to:

7.1.1 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

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

7.1.3 Receive results in one or more of the following methods stated as a preference by the Authorized User:

- 7.1.3.1 Directly into the Authorized User's EMR/EHR or other third party software
- 7.1.3.2 For viewing in a QE's clinical viewer
- 7.1.3.3 As a secure message at a designated address, including an email inbox

7.1.4 Methods and preferences other than viewing in the QE's clinical viewer are supported providing that all of the following conditions are met:

- 7.1.4.1 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
- 7.1.4.2 QE Authorized Users request testing and supporting results delivery to the third party software or a secure message system address, and testing and supporting interface is economically feasible and sustainable for the QE; third party software and Direct interfaces are supported at the QE's discretion

7.2 QE Certification Requirements

To enable results delivery, QEs must:

7.2.1 Detect results from within HL7 messages received from source systems

7.2.2 Conform to standards and specifications established by the Statewide PRL: Statewide MPI (sMPI) and PRL (sPRL) Functional Specification

7.2.3 Results are routed to the specified end-point within a set length of time from receipt by the QE, as defined by the local QE

7.3 QE Service Level Requirements for Certification

Conformance to service levels for reliability and availability of user requirements as outlined in Service Level Agreements (SLAs) between a QE and their Participants.

8. Public Health Integration

Public Health Integration services aim to support the Public Health reporting services to State, local, and city Public Health agencies. Such services include: immunizations; syndromic surveillance data; reportable laboratory results; cancer cases; disaster tracking during declared state of emergency events; and newborn bloodspot screening.

8.1 User Requirements

Through public health integration services available from the QE, an Authorized User must be able to:

8.1.1 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.

8.1.2 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 8.2.4

8.2 QE Certification Requirements

To enable public health integration, QEs must:

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

8.2.2 Enable public health role-based queries of individual patient records, as defined and approved pursuant to the Statewide PRL: Statewide MPI (sMPI) and PRL (sPRL) Functional Specification and the SHIN-NY Policies and Procedures

8.2.3 Log all public health access as required by the SHIN-NY Policies and Procedures

8.2.4 QE must, when requested by Public Health Agencies, provide the following public health reporting services for an authorized Public Health Agency based on reporting requirements outlined by Public Health Agencies and in conjunction with NYS DOH and NYC DOHMH.

- 8.2.4.1 Syndromic surveillance data – to NYS DOH and NYC DOHMH
- 8.2.4.2 Reportable laboratory results – to NYS DOH and NYC DOHMH
- 8.2.4.3 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 SHIN-NY Policies and Procedures
- 8.2.4.4 Immunizations – to NYS DOH and the New York City Department of Health and Mental Hygiene (NYC DOHMH) as per specific DOH and/or DOHMH requirements
- 8.2.4.5 Cancer cases – to the NYS DOH Cancer registry as per Cancer registry requirements
- 8.2.4.6 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
- 8.2.4.7 Other areas of reporting requested by NYS DOH or NYC DOHMH as allowed by law and policy.

8.2.5 Ability to queue or otherwise store reporting messages in the event of an outage, so messages can be sent when either the sending QE or receiving public health end-point

becomes available again

8.2.6 Ability to pass through acknowledgements and verification messages as required by the public health reporting services to which the QE is connected

8.3 QE Service Level Requirements for Certification

Conformance to service levels for reliability and availability of user requirements as outlined in Service Level Agreements (SLAs) between a QE and their Participants.