Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1)

Version 4.2

REVISED January 2025

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

TABLE OF CONTENTS

Introduction. This document, the Privacy and Security Guidance for Qualified Entities and their Participants provides information related to privacy and security for Qualified Entities participating in New York's Statewide Health Information Network, consistent with 10 N.Y.C.R.R. § 300.3(b)(1). This guidance ensures secure health information exchange through the Statewide Health Information Network for New York (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 this guidance, which is compliant with all applicable state and federal laws.

Process for Amending Guidance. NYS DOH may update and/or amend the guidance based on recommendations solicited through the Statewide Collaboration Process (SCP). Recommendations and proposed changes will be developed, shared with stakeholders and amended on an as needed basis and will be incorporated into this guidance document and posted on NYS DOH's website.

Target Audience. Qualified Entities (QEs), their participants, the New York State Department of Health, and contributors of data to the SHIN-NY are the intended audience for this guidance, which provides information to assure QE compliance with rules and regulations and to promote statewide interoperability and exchange of health information.

Definitions.

Access means the ability of an Authorized User or Certified Application to view Protected Health Information on a QE's electronic health information system following the Authorized User's or Certified Application's logging on to such QE.

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.

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) an Alternative Consent; or (iv) a consent that may be relied upon under the Patient Consent Transition Rules set forth in Section 1.10.

Alternative Consent means a consent form approved under Section 1.3 as an alternative to a Level 1 Consent or a Level 2 Consent.

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 1.10.

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

Authenticator Assurance Level 2 (AAL2) means the authentication categorization set forth in NIST SP 800-63 which provides high confidence that the individual seeking access controls authenticator(s) bound to the Authorized User's account. Under AAL2, proof of possession and control of two distinct authentication factors are required through secure authentication protocol(s).

Authorized User means an individual who has been authorized by a Participant or a QE to Access patient information via the SHIN-NY in accordance with these 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; (iii) 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 1.2.4.

Business Associate Agreement means a written signed agreement meeting the HIPAA requirements of 45 C.F.R. § 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, (iv) supporting a patient in following a plan of medical care, or (v) assisting a patient in obtaining social services or providing social services to a patient.

CARIN Alliance means the multi-sector collaborative that seeks to advance consumer-directed exchange of health information and which has developed a list of recommended Patient Apps via its "My Health Application" website.

Centralized Research Committee means a committee that includes representatives of all QEs in the SHIN-NY that is organized to review and approve Research proposals under which a researcher seeks information from more than one QE. The Centralized Research Committee shall meet the requirements set forth at 45 C.F.R. § 164.512(i)(1)(i)(B), meaning that the committee (1) has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the Research protocol on individuals' privacy rights and related interests; (2) includes at least one member who is not an employee, contractor, officer or director of a QE or any entity conducting or sponsoring the research, and is not related to any person who meets any of the foregoing criteria; and (3) does not have any member participating in a review of any project in which the member has a conflict of interest.

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.

Community-Based Organization means an organization, which may be a not-for-profit entity or government agency, which has the primary purpose of providing social services such as housing assistance, nutrition assistance, employment assistance, or benefits coordination. A Community-Based Organization may or may not be a Covered Entity.

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.

Coroner means any individual elected to serve as a county's coroner in accordance with New York State County Law § 400.

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.

Cybersecurity Policies and Procedures (CSPP) means the QE's and the State Designated Entities' set of policies and procedures that aim to protect the QE and SHIN-NY Enterprise's information systems and data.

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 (such as clinical laboratories and pharmacies). Government agencies, including Public Health Agencies, may be Data Suppliers.

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.

Disaster Relief Agency means (i) a government agency with authority under federal, state or local law to declare an Emergency Event or assist in locating individuals during an Emergency Event or (ii) a third-party contractor to which such a government agency delegates the task of assisting in the location of individuals in such circumstances.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. A QE engages in a Disclosure of information if the QE (i) provides a Participant with Access to such information and the Participant views such information as a result of such Access, or (ii) Transmits such information to a Participant or other third party.

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.

Emergency Event means a circumstance in which a government agency declares a state of emergency or activates a local government agency incident command system or similar crisis response system.

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 and 800.6 as an emergency medical technician, an emergency medical technician-intermediate, an emergency medical technician-critical care, or an emergency medical technician-paramedic.

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.

Health Information Exchange Organization means an entity that facilitates and oversees the exchange of Protected Health Information among Covered Entities, Business Associates, and other individuals and entities.

Health Oversight Agency has the meaning ascribed to this term in 45 C.F.R. § 164.501.

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

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

HIPAA Security Rule means the federal regulations at 45 C.F.R. 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).

Information Blocking Rules means the requirements and exceptions related to information blocking established by The Office of the National Coordinator for Health Information Technology set forth at 45 C.F.R. Part 171.

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 and receipt of Protected Health Information for Level 1 Uses in one of the forms attached hereto as Appendix A.

Level 2 Consent means a consent permitting Access to and receipt of Protected Health Information for a Level 2 Use in one of the forms attached hereto as Appendix B.

Level 1 Uses mean Treatment, Quality Improvement, Care Management, Utilization Review, 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.

Limited Data Set means Protected Health Information that excludes the 16 direct identifiers set forth at 45 C.F.R. § 164.514(e)(2) of an individual and the relatives, employers or household members of such individual.

Marketing has the meaning ascribed to this term under the HIPAA Privacy Rule as amended by Section 13406 of HITECH (42 USC § 17936).

Medical Examiner means a licensed physician who serves in a county medical examiner's office in accordance with New York State County Law § 400, and shall include physicians within the New York City Office of Chief Medical Examiner.

Minor Consent Services means those services for which a minor may provide their own consent without a parent's or guardian's permission, as permitted by New York State law, including but not limited to services provided pursuant to Public Health Law sections 2305 and 2504 and Mental Hygiene Law sections 22.11 and 33.21, or other applicable laws for certain types of health services (e.g., reproductive health, HIV testing, STD, mental health or substance use treatment) or services consented to by an Emancipated Minor.

National Institute of Standards and Technology (NIST) Cybersecurity Framework means the set of industry standards and best practices to help organizations manage cybersecurity risks that has been developed by the National Institute of Standards and Technology. The NIST

Cybersecurity Framework uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

NYS DOH means the New York State Department of Health.

One-to-One Exchange means a Transmittal of Protected Health Information originating from a Participant which has a relationship with a patient to one or more other Participants with the patient's knowledge and implicit or explicit consent where no records other than those of the Participants jointly providing health care or social services to the patient are Transmitted. Examples of a One-to-One Exchange include, but are not limited to, information provided by a primary care provider to a specialist when referring to such specialist, a discharge summary sent to where the patient is transferred, lab results sent to the Practitioner who ordered the laboratory test, or a claim sent from a Participant to the patient's health plan.

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 (42 USC § 1320b-8[b]; see also 42 C.F.R. Part 121).

Participant means a Provider Organization, Payer Organization, Practitioner, Independent Practice Association, Accountable Care Organization, Public Health Agency, Organ Procurement Organization, Health Home, Health Home Member, Performing Provider System (PPS) Partner, PPS Lead Organization, PPS Centralized Entity, Social Services Program, Community-Based Organization, Social Care Network Lead Entity, or Disaster Relief Agency that has directly or indirectly entered into a Participation Agreement with a QE and Accesses Protected Health Information via the SHIN-NY.

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 App means an application on a patient's smart phone, laptop, tablet, or other technology that collects Protected Health Information about the patient and makes such Protected Health Information accessible to the patient.

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 Transmitted 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 Care Alerts may contain demographic information such as patient name and date of birth, the name of the Participant from which the patient received treatment, and limited information related to the patient's complaint or diagnosis but shall not include the patient's full medical record relating to the event that is the subject of the electronic message.

Patient Consent Transition Rules means the rules set forth in Section 1.10.

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 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 the Employee Retirement Income Security Act of 1974 (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 the professional 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, the New York State Department of Health, a New York county health department or the New York City Department of Health and Mental Hygiene, 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.

QE Research Committee means a committee of a QE that is organized to review and approve Research proposals and which meets the requirements set forth at 45 C.F.R. § 164.512(i)(1)(i)(B), meaning that the committee (i.) has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the Research protocol on individuals' privacy rights and related interests; (ii.) includes at least one member who is not an employee, contractor, officer or director of the QE or any entity conducting or sponsoring the research, and is not related to any person who meets any of the foregoing criteria; and (iii.) does not have any member participating in a review of any project in which the member has a conflict of interest.

Qualified Entity Participation Agreement (QEPA) means the agreement between each of the QEs and the State Designated Entity that sets forth the terms and conditions for the QE participation in the SHIN-NY including providing QE Participants Access to and use of the SHIN-NY.

Qualified 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 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, that can be queried 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.

Retrospective Research means Research that is not conducted in connection with Treatment and involves the use of Protected Health Information that relates to Treatment provided prior to the date on which the Research proposal is submitted to an Institutional Review Board.

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 use, reproductive health, sexually transmitted disease, and genetic testing information.

SHIN-NY means the technical infrastructure (SHIN-NY Enterprise) and the supportive policies and agreements that make possible the electronic exchange of clinical information among QEs, Participants, and other individuals and entities for authorized purposes, including both the infrastructure that allows for exchange among Participants participating in the same QE and the infrastructure operated by the State Designated Entity that allows for exchange between different QEs. The goals of the SHIN-NY are to improve the quality, coordination, and efficiency of patient care, reduce medical errors and carry out public health and health oversight activities, while protecting patient privacy and ensuring data security.

SHIN-NY Enterprise means the information technology (IT) infrastructure inclusive of the Qualified Entities (QEs) and the Statewide Data Infrastructure that supports the electronic exchange of patient health information across New York State.

Social Care Network Lead Entity means an entity that is responsible under a contract with NYS DOH for establishing a network inclusive of Community-Based Organizations providing health-related social needs services to Medicaid enrollees as originally established as part of the New York Health Equity Reform (NYHER) program.

Social Services Program means a program within a social services district (as defined by New York Social Services Law, § 2) which has authority under applicable law to provide "public assistance and care" (as defined by New York Social Services Law § 2), Care Management, or

coordination of care and related services.

sPRL means Statewide Patient Record Lookup, a system under which Protected Health Information or other information may be accessed across QE systems for disclosure to a Participant or other person who is permitted to receive such information under the terms of these Policies and Procedures.

State Designated Entity (SDE) means the public/private partnership in New York State that has been designated by the New York State Commissioner of Health as eligible to receive federal and state grants to promote health information technology.

Statewide Chief Information Security Officer (CISO) means the senior-level executive employed by the State Designated Entity who has authority over the SHIN-NY Enterprise in order to establish and maintain the vision, strategy, and security program to ensure the SHIN-NY Enterprise's information assets and technologies are adequately protected.

Statewide Consent Date means the date or dates established via the Statewide Collaboration Process by which Participants must offer to patients the Statewide Form of Consent.

Statewide Consent Management System means a system designed to track patient responses for Consent, including modifications to prior consent choices, and share those responses with QEs and Participants.

Statewide Data Infrastructure means the information technology infrastructure operated by or for the State Designated Entity that supports the aggregation of data provided by QEs and Participants, statewide reporting and analytics for public health activities and Medicaid purposes, and the exchange of information between QEs.

Statewide Form of Consent means the statewide Level 1 Consent that at minimum, allows for disclosure of Protected Health Information to all current and future Participants who provide Treatment to a patient, regardless of which QE such Participants have contracted with.

Telehealth means the use of electronic information and two-way, real-time communication technologies to deliver health care to patients at a distance. Such communication technologies include both audio-video and audio-only (e.g., telephonic) connections.

Transmittal means the sharing of Protected Health Information, a Limited Data Set, or De-identified Data to a recipient in either paper or electronic form, other than via the display of such information through the QE's electronic health information system or through a Certified Application.

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 (42 USC 17932[h][2]).

Utilization Review means an activity carried out by a Payer Organization to determine whether a health care item or service that has been provided to an enrollee of such Payer Organization, or which has been proposed to be provided to such an enrollee, is medically necessary. *This policy is not intended to supersede or affect any state or federal laws related to Utilization Review. (See NY Insurance Law §4900(h) and Public Health Law §4900(8)).*

SECTION 1: CONSENT

Purpose/Principles

The purpose of this guidance is to ensure processes are in place to gather and document patient consent, and that the privacy and security of patients' Protected Health Information remains secure while facilitating the sharing of such information to provide better quality health care.

Policies and Procedures

1.1 Requirement to Obtain Affirmative Consent. Except as set forth in Section 1.2, a QE shall not Disclose a patient's Protected Health Information via the SHIN-NY to a Participant unless the patient has provided an Affirmative Consent authorizing the Participant to Access or receive such Protected Health Information. An Affirmative Consent may be executed by an electronic signature as permitted by Section 1.9.5.

1.2 Exceptions to Affirmative Consent Requirement. Affirmative Consent shall not be required under the circumstances set forth in this Section 1.2. As required by Section 1.2, Disclosures of Protected Health Information without Affirmative Consent shall comply with applicable federal, state and local laws and regulations, including 42 C.F.R. Part 2. Protected Health Information subject to 42 C.F.R. Part 2 shall not be Disclosed without Affirmative Consent unless 42 C.F.R. Part 2 specifically allows for such Disclosure.

1.2.1 One-to-One Exchanges. Affirmative Consent shall not be required for a Transmittal of a patient's Protected Health Information originating from one Participant to another Participant if such Transmittal meets all the requirements of a One-to-One Exchange (including the requirement that the Transmittal occur with the patient's implicit or explicit consent) provided the Participants comply with existing federal and state laws and regulations requiring patient consent for the Disclosure and re-disclosure of information by health care providers.[1] If Protected Health Information is Transmitted to a Payer Organization under a One-to-One Exchange, such exchange must comply with Section 1.9.13 which allows an individual to request a restriction on the Disclosure of Protected Health Information.

1.2.2 Public Health Reporting and Access.

a. 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),

[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.*

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.

b. A QE may Disclose Protected Health Information to a Public Health Agency without Affirmative Consent for public health activities authorized by law, including:

i. To investigate suspected or confirmed cases of communicable disease (pursuant to PHL § 2[1][l] and 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. As authorized by PHL § 206(1)(d) to investigate the causes of disease, epidemics, the sources of mortality, and the effect of localities, employments and other conditions, upon the public health, and by PHL § 206(1)(j) for scientific studies and research which have for their purpose the reduction of morbidity and mortality and the improvement of the quality of medical care through the conduction of medical audits;

v. For purposes allowed by Article 21, including Article 21, Title 3 and 10 N.Y.C.R.R. Part 63 (HIV) and Article 21, Title 6 and 10 N.Y.C.R.R. Part 66 (immunizations);

vi. For purposes allowed by PHL § 2(1)(n), Article 23 and 10 N.Y.C.R.R. Part 23 (STD).

vii. For purposes allowed by PHL § 2401 and 10 N.Y.C.R.R. § 1.31 (cancer);

viii. For the activities of the Electronic Clinical Laboratory Reporting System (ECLRS), the Electronic Syndromic Surveillance System (ESSS), the Health Emergency Response Data System (HERDS), and the Statewide Planning and Research Cooperative System (SPARCS);

ix. For purposes allowed by PHL § 2004 and 10 N.Y.C.R.R. Part 62 (Alzheimer's);

x. For purposes allowed by PHL § 2819 (infection reporting);

xi. For quality improvement and quality assurance under PHL Article 29-D, Title 2, including quality improvement and quality assurance activities under PHL § 2998-e (office-based surgery);

xii. For purposes allowed under 10 N.Y.C.R.R. Part 22 (environmental diseases);

xiii. To investigate suspected or confirmed cases of lead poisoning (pursuant to 10 N.Y.C.R.R. Part 67);

xiv. For purposes allowed by 10 N.Y.C.R.R. Part 69 (including newborn disease screening, newborn hearing screening and early intervention);

xv. For purposes allowed under 10 N.Y.C.R.R. § 400.22 (Statewide Perinatal Data System);

xvi. For purposes allowed under 10 N.Y.C.R.R. § 405.29 (cardiac data); or

xvii. For any other public health activities authorized by law. "Law" means a federal, state or local constitution, statute, regulation, rule, common law, or other governmental action having the force and effect of law, including the Charter, Administrative Code and Rules of the City of New York.

c. QEs may Disclose Protected Health Information without Affirmative Consent to the New York State Office of Mental Health ("OMH") for the following public health purposes if such QE Discloses Protected Health Information to NYS DOH in its role as a Public Health Agency and OMH is authorized to obtain such information under applicable state and federal law. Such public health purposes shall consist of investigations aimed at reducing morbidity and mortality, monitoring of disease trends, and responding to public health emergencies.

d. A patient's denial of consent for all Participants in a QE to Access the patient's Protected Health Information under Section 1.9.6 shall not prevent or otherwise restrict a QE from Disclosing to a Public Health Agency the patient's Protected Health Information through a QE for the purposes set forth in Section 1.2.2(b)(i)-(xvii).

e. A QE may Disclose the reports and information subject to 10 N.Y.C.R.R. §63.4 (HIV clinical laboratory test results), for purposes of linkage to and retention in care, to Participants engaged in Care Management that have a clinical, diagnostic, or public health interest in the patient, to the extent permitted under 10 N.Y.C.R.R. §63.4(c)(3). Participants engaged in Care Management with a clinical, diagnostic, or public health interest in a patient may include, but are not limited to, Provider Organizations or Practitioners

with a Treatment relationship with a patient, Health Homes, and Payer Organizations providing Care Management to their enrollees. A QE shall work in consultation with the New York State Department of Health, AIDS Institute, prior to implementing any program under this provision.

1.2.3 Disclosures for Disaster Tracking.

a. For the purpose of locating patients during an Emergency Event, a QE may Disclose to a Disaster Relief Agency the following information without Affirmative Consent:

i. Patient name and other demographic information in accordance with the principles set forth in Section 4.6;

ii. Name of the facility or facilities from which the patient received care during the Emergency Event; dates of patient admission and/or discharge.

b. A QE may Disclose information under this section during an Emergency Event only.

c. Information Disclosed under this section shall not reveal the nature of the medical care received by the patient who is the subject of the Disclosure unless the Governor of New York, through Executive Order, temporarily suspends New York State health information confidentiality laws that would otherwise prohibit such Disclosure, as authorized under N.Y. Executive Law Section 29-a.

d. A patient's denial of consent for all Participants in a QE to Access or receive the patient's Protected Health Information under Section 1.9.6 shall not restrict a QE from Disclosing information to a Disaster Relief Agency as permitted by this section.

1.2.4 Emergency Disclosures of Protected Health Information When Treating a Patient with an Emergency Condition or "Breaking the Glass."

a. Affirmative Consent shall not be required for a QE to Disclose Protected Health Information to (i) a Practitioner; (ii) an Authorized User acting under the direction of a Practitioner; or (iii) an Emergency Medical Technician, 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 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 Emergency Medical Technician determines, in such individual's reasonable judgment, that information that may be held by or accessible via the SHIN-NY may be material to emergency treatment. The individual "Breaking the Glass" may do so in a facility, an ambulance, or another location, provided that such individual accesses Protected Health Information only after the determination in subsection (a)(i) has been made.

iii. No denial of consent to Access or receive 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 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, 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 Disclosure.

b. Emergency Protected Health Information 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 Disclosures pursuant to this Section 1.2.4 do not occur after 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 Disclosure where the circumstances set forth in this Section 1.2.4 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 Disclosed under this Section 1.2.4. This notice shall include (i) the name of the Participant that received the Protected Health Information; (ii) the name of the Authorized User within the Participant that received the Protected Health Information; (iii) the date and time of the Disclosure; and (iv) the nature of the emergency.

f. If a Participant accesses Protected Health Information under this Section 1.2.4, the Participant shall notify the patient of such incident and inform the patient how they may request an Audit Log in accordance with Section 6.4 of these Policies and Procedures. In lieu of providing such notice, Participants that are hospitals may notify all patients discharged from an

emergency room that their Protected Health Information may have been Disclosed during a Break the Glass incident and inform patients how they may request an Audit Log to determine if such Disclosure occurred. The notice required by this Section shall be provided within ten days of the patient's discharge (or, in the case of access that does not relate to a hospital admission, within ten days of the date of such access) and may be provided by the QE on behalf of the Participant.

1.2.5 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 Disclose the information until Affirmative Consent is obtained, except as otherwise permitted in these Policies and Procedures.

1.2.6 QE Access for Operations and Other Purposes.

a. Affirmative Consent shall not be required for a QE or its contractors to Access or receive Protected Health Information via the SHIN-NY to enable the QE to perform system maintenance, testing and troubleshooting and to provide similar operational and technical support.

b. Affirmative Consent shall not be required for a QE or its contractors to Access or receive Protected Health Information via the SHIN-NY at the request of a Participant in order to assist the Participant in carrying out activities for which the Participant has obtained the patient's Affirmative Consent. Such Access or receipt must be consistent with the terms of the Business Associate Agreement entered into by the Participant and the QE.

c. Affirmative Consent shall not be required for a QE, government agencies or their contractors to Access or receive Protected Health Information via the SHIN-NY for the purpose of evaluating and improving QE operations.

1.2.7 De-Identified Data. Affirmative Consent shall not be required for a QE to Disclose De-identified Data for specified uses as set forth in Section 1.6.

1.2.8 Organ Procurement Organization Access. A QE may Disclose Protected Health Information to an Organ Procurement Organization 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 1.9.6 shall not prevent or otherwise restrict an Organ Procurement Organization from Accessing or receiving the patient's Protected Health Information through a QE for the purposes set forth in this Section 1.2.8.

1.2.9 Patient Care Alerts.

a. A Patient Care Alert may be Transmitted to a Participant without Affirmative Consent provided that the recipient of such Patient Care Alert is a Participant that provides, or is responsible for providing, Treatment or Care Management to the patient. Such categories of Participants may include, but are not limited to, Practitioners, Accountable Care Organizations, Health Homes, Payer Organizations, PPS Centralized Entities, PPS Partners, and home health agencies who meet the requirements of the preceding sentence. If a patient or a patient's Personal Representative affirmatively denies consent to a Participant to Access the patient's information, then Patient Care Alerts shall not be Transmitted to such Participant.

b. Patient Care Alerts may be Transmitted from facilities subject to the New York Mental Hygiene Law without Affirmative Consent only if such alerts are sent to Payer Organizations, Health Homes, or other entities authorized by the New York State Office of Mental Health and the sending of such alerts otherwise complies with Mental Hygiene Law § 33.13(d).

c. Patient Care Alerts shall be Transmitted in an encrypted form that complies with U.S. Department of Health and Human Services "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals".

1.2.10 Disclosures to Payer Organizations for Quality Measures. Affirmative Consent shall not be required for a QE to Disclose Protected Health Information to a Payer Organization (including NYS DOH in regards to its operation of the New York State Medicaid program) or a Business Associate of a Payer Organization to the extent such Disclosure is necessary to (i) calculate performance of HEDIS or QARR measures; or (ii) in the case of disclosures to NYS DOH, determine payments to be made under the New York State Medicaid program or to evaluate services or initiatives, determine trends, or coordinate care under the Medicaid program, to the extent permitted by the HIPAA Privacy Rule.

1.2.11 Death Notifications. Affirmative Consent shall not be required for a QE to Disclose the death of a patient to a Participant that (a) was responsible for providing Treatment or Care Management to such patient prior to the patient's death; or (b) is a Payer Organization that provided health coverage to the patient immediately prior to the patient's death. A death notification may only include Demographic Information and the date and time of death. Cause of death and information on the patient's diagnoses, health conditions, and treatments, as well as location of death, shall not be included in the death notification absent Affirmative Consent.

1.2.12 Disclosures to Death Investigators. Affirmative Consent shall not be required for a QE to Disclose Protected Health Information to a Participant for the purposes of determining the cause of a patient's death provided that all of the following are met:

a. The individual accessing or receiving the Protected Health Information is a licensed physician or nurse practitioner whose professional responsibilities include determining the cause of death of a patient, or an individual acting under the supervision of such Practitioner. Such individuals may include Medical Examiners and Coroners who are licensed as physicians or nurse practitioners, or an individual acting under the supervision of such a Medical Examiner or Coroner.

b. The QE and the Participant abide by the minimum necessary standard set forth at Section 4.5.

c. Protected Health Information originating from a facility subject to the New York Mental Hygiene Law is Disclosed only if the facility has requested that an investigation be conducted into the death of a patient and the recipient is a Medical Examiner or Coroner that is licensed as physician or nurse practitioner.

d. The QE, either directly or from one of its Participants, has received an attestation that includes all the elements set forth in 45 C.F.R. § 164.509, to the extent such attestation is required by the HIPAA Privacy Rule.

1.2.13 Telehealth.

a. General. Affirmative Consent shall not be required for a QE to disclose a patient's Protected Health Information to a Participant that provides telehealth services to such patient if:

i. The Participant has asked the patient if the Participant may Access or receive the patient's Protected Health Information, and the patient has verbally consented to such request;

ii. The Participant uses the Protected Health Information only for Level 1 purposes;

iii. The Participant keeps a record of the patient having provided verbal consent, which may take the form of a notation in the electronic record of such consent, an audio recording of the consent, or another appropriate means of recording consent;

iv. The Participant does not Access or receive any Protected Health Information subject to 42 C.F.R. Part 2 or Mental Hygiene Law § 33.13 unless the patient has provided consent in written or electronic form and a signature that is recognized by the Electronic Signatures and Records Act, including an audio signature recording to the extent recognized under that act; and

v. The Participant Accesses or receives the patient's Protected Health Information only during the time period specified in subsection b.

b. Duration of Telehealth Verbal Consent. The patient's verbal consent

shall remain valid until the patient has an in-person encounter with the Participant or revokes consent, provided that the Participant:

i. Informs the patient that the consent will persist until the patient an in-person encounter with the Participant or revokes consent;

ii. Informs the patient of the patient's right to revoke consent by notifying the Participant of such revocation either verbally or in writing; and

iii. Provides the patient with access to a written consent form that documents the terms of the verbal consent by either providing the patient with a copy of the form (via email, text, mail or otherwise) or an electronic link to such form.

The Participant shall keep a record of having provided such information to the patient. If the Participant fails to comply with requirements (i) through (iii) above, the verbal consent shall remain valid only for 72 hours.

c. Applicability to Electronic Consents. If a Participant obtains the patient's electronic signature, including a recording of oral consent, that is recognized by the Electronic Signatures and Records Act, then such consent shall be governed by Section 1.9.5 and shall not be subject to the requirements of this section.

1.2.14 Utilization Review Requirements. In the event a QE permits a Payer Organization to Access or receive Protected Health Information for Utilization Review purposes in accordance with an individual's Affirmative Consent, such QE shall require the Payer Organization to, prior to denying coverage of an item or service based on Utilization Review, (a) notify the Provider Organization whose item or service is subject to the Utilization Review activity that such Payer Organization has reviewed the Provider Organization's Protected Health Information in the SHIN-NY; and (b) offer to provide the Provider Organization with a copy of the Protected Health Information so reviewed. In addition, the QE shall require the Payer Organization to provide notice to its contracted Provider Organizations, whether through contractual terms, policies, or otherwise, that such Payer Organization may access the Provider Organization's Protected Health Information in the SHIN-NY. *This policy is not intended to supersede or affect any state or federal laws related to Utilization Review. (See NY Insurance Law §4900(h) and Public Health Law §4900(8).*

1.3 Form of Patient Consent. Consents shall be obtained through an Approved Consent. A QE may approve an alternative to a Level 1 Consent or a Level 2 Consent if the Alternative Consent includes the information specified in this section and, if the form is an alternative to a Level 1 Consent, the QE is permitted to recognize the form in accordance with Section 1.3.5. As required by Section 1.9.12, QEs are responsible for ensuring that any approved Alternative Consents comply with applicable federal, state, and local laws and regulations. If an Alternative Consent is to be used as a basis for exchanging information subject to 42

C.F.R. Part 2, the QE shall ensure that such form meets the requirements of 42 C.F.R. Part 2

1.3.1 Level 1 Uses. Affirmative Consent to Access or receive information via the SHIN-NY for Level 1 Uses shall be obtained using a Level 1 Consent or an Alternative Consent approved by a QE under this Section 1.3.1, which shall include the following information:

a. A description of the information which the Participant may Access or receive, including specific reference to HIV, mental health, alcohol and substance use, reproductive health, sexually transmitted disease, and genetic testing information, if such categories of information may be Disclosed to the recipient.

b. The Participant's intended uses for the information. A general description, such as "for treatment, care management or quality improvement," shall meet this requirement.

c. The name(s) or description of both the source(s) and potential recipient(s) of the patient's information. A general description, such as "information may be exchanged among providers that provide me with treatment," shall meet this requirement.

d. The signature of the patient or the patient's Personal Representative. If the consent language required under subsections (a), (b), and (c) above is incorporated into another document such as a health insurance enrollment form in accordance with Section 1.3.3(c), the signature need not appear on the same page as the language required under subsections (a), (b), and (c) above.

1.3.2 Level 2 Uses. Consent to Access or receive information via the SHIN-NY for the purposes of Level 2 Uses shall be obtained using a Level 2 Consent or an Alternative Consent approved by a QE under this Section 1.3.2, which shall include (i) the information required pursuant to Section 1.3.1 and (ii) the following information:

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

b. Whether the QE and/or its Participants will benefit financially as a result of the Disclosure of the patient's information;

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;

e. 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;

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

g. Whether and to what extent information is subject to re-disclosure; and

h. The date of execution of the 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 a QE. If a QE agrees to allow an Alternative Consent that is combined with a health insurance enrollment form, such Alternative Consent shall expire no later than the date on which the patient's health insurance enrollment terminates.

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 or receive Protected Health Information via the SHIN-NY for the purpose of Marketing, the QE or its Participant must provide the patient with information about the nature of such Marketing.

1.3.5 Naming of QEs and Recognition of Consents.

a. QEs shall permit the Disclosure of Protected Health Information based on an individual's execution of an affirmative consent.

b. QEs may permit the Disclosure of Protected Health Information based on a Level 1 Alternative Consent executed only if:

i. The Alternative Consent has been approved and issued by a New York State agency;

ii. The Alternative Consent was obtained by a hospital Participant, or a Provider Organization Participant that uses such Alternative Consent in multiple states, and such Participant used such Alternative Consent prior to the Statewide Consent Date;

iii. The Alternative Consent permits Disclosures to a Participant that is not included among the potential recipients of Protected Health Information under the SHIN-NY Consent; or

iv. The Alternative Consent was obtained by an individual or entity that is not a Participant in any QE.

Nothing herein limits the ability of QEs to recognize a Level 1 Alternative Consent or a Level 2 Alternative Consents executed either before or after the Consent Implementation Date.

c. An Affirmative Consent form is not required to include the name of a QE.

d. Up until a date to be determined by NYS DOH, a QE may continue to use an Affirmative Consent form on which the name of such QE appears.

e. In the case where an Affirmative Consent form does not include the name of a particular QE, such QE shall Disclose to a Participant a patient's Protected Health Information even if such QE's name does not appear on the Affirmative Consent form so long as:

i. the patient signed the Affirmative Consent form;

ii. the Affirmative Consent form names the Participant or indicates that Protected Health Information may be disclosed to a class of Participants (for example, treating providers) that includes the Participant in accordance with Section 1.3.1(c); and

iii. the Disclosure otherwise complies with these Policies and Procedures.

1.3.6 Statewide Consent and Statewide Consent Management

a. As of the Statewide Consent Date, Participants shall offer to their patients the Statewide Form of Consent.

b. The State Designated Entity shall operate the Statewide Consent Management System. QEs shall coordinate with the State Designated Entity to ensure that Protected Health Information is used and disclosed in the SHIN-NY in accordance with patient choices made on the Statewide Form of Consent and as recorded in the Statewide Consent Management System.

1.3.7 Expiration at Death. In the event an Affirmative Consent indicates the consent expires upon an individual's death, a QE may disclose Protected Health Information in accordance with the terms of the Affirmative Consent until the QE reasonably determines, based on record(s) received from Participants or government agencies, that the individual has died, provided the QE undertakes reasonable efforts to collect records indicating date of death.

1.4 Sensitive Health Information.

1.4.1 General. An Affirmative Consent may authorize the Participant(s) listed in the consent to Access or receive 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 Disclosure. In the event that a QE or a Participant has provided a patient the option to withhold certain pieces of Sensitive Health Information from Disclosure, and the patient has exercised that option, the patient's record may, but is not required to, carry an alert indicating that data has been withheld from the record.

1.4.3 Re-disclosure Warning.

a. QEs shall include a warning statement that is viewed by Authorized Users whenever they are obtaining Access to or receiving Transmittals of 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 re-disclosure 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 or receiving Transmittals of HIV/AIDS information protected under Article 27-F of the N.Y. Public Health Law that contains the language required by Article 27-F (see Public Health Law § 2782[5]). A QE may satisfy this requirement by (i) placing such a re-disclosure warning on the same screen on which it places the re-disclosure 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 or receiving Transmittals of 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 re-disclosure 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 Sensitive Health Information in order to ensure compliance with applicable state and federal laws and regulations governing re-disclosure of such information, including, but not limited to, those applicable to HIV/AIDS, alcohol and substance use 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 A Participant may Access or receive Protected Health Information about minors -

other than information regarding Minor Consent Services - based on an Affirmative Consent executed by the minor's Personal Representative.

1.5.2 A Participant may Access or receive information regarding Minor Consent based on an Affirmative Consent executed by the minor's Personal Representative unless federal or state law or regulation requires the minor's authorization for such Disclosure, in which case a Participant may not Access or receive such information without the minor's Affirmative Consent.

1.5.3 Notwithstanding Section 1.5.2, QEs and their Participants may not disclose information regarding Minor Consent Services to the minor's Personal Representative without the minor's written consent.

1.6 De-Identified Data.

1.6.1 A QE may Disclose De-Identified Data without Affirmative Consent if the QE enters into a data use agreement with the recipient in accordance with Section 1.6.3, unless the QE determines that (a) such De-Identified Data is to be used to assist in Marketing activities that would not comply with the HIPAA Privacy Rule, or (b) the proposed use of the De-Identified Data is not in keeping with the mission of the SHIN-NY as described in 10 N.Y.C.R.R. § 300.1. Notwithstanding the foregoing, a data use agreement shall not be required if the QE solely is Transmitting to a third party that is designing a clinical trial or other clinical research study a count of the number of patients who appear to meet the inclusion and/or exclusion criteria being considered for such clinical trial or study, so long as there is no reasonable basis to believe that the count, when combined with the qualifying criteria, can be used to identify an individual.

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

1.6.3 A QE shall ensure that a data use agreement required under this Section 1.6:

a. Establishes the permitted uses of the De-Identified Data by the recipient and prohibits the recipient or any third parties from using the De-Identified Data for any purposes other than the permitted uses, unless otherwise required by law.

b. Prohibits the recipient from re-identifying or attempting to re-identify the De-Identified Data.

c. Provides the QE, or a Participant who holds Protected Health Information that was used in whole or in part to create the De-Identified Data set, with a right to audit the practices of the recipient regarding ensuring the data is not re-identified.

d. Requires the recipient to report to the QE if the recipient has knowledge that the De-Identified Data has been re-identified or if there have been any other violations of the data use agreement.

e. Mandates that the recipient may not disclose the De-Identified data to any third party unless the agreement explicitly permits such a Disclosure, and the third party also agrees in writing to follow the restrictions set forth in this Section 1.6.3.

1.6.4 Any Disclosures of De-Identified Data shall comply with any applicable terms in the Business Associate Agreement between the QE and the Data Suppliers that are the source of the De-Identified Data.

1.7 Research.

1.7.1 Research Involving De-Identified Data. Affirmative Consent shall not be required for a QE to Disclose De-Identified Data for purposes of Research, provided that a QE has adopted policies that inform Data Suppliers about the circumstances under which De-Identified Data may be Disclosed and the QE enters into a data use agreement with the researcher that meets the requirements of Section 1.6.3. The Disclosure of De-Identified Data under this section is subject to the QE's compliance with policies adopted by the QE, which set forth criteria that will be utilized to determine when a proposed Disclosure under this section must be approved by an Institutional Review Board or QE Research Committee.

1.7.2 Research Involving a Limited Data Set. Affirmative Consent shall not be required for a QE to Disclose a Limited Data Set for purposes of Research, provided that (i) a QE has adopted policies that inform Data Suppliers about the circumstances under which a Limited Data Set may be Disclosed; and (ii) a QE enters into a data use agreement with the researcher prior to Disclosing the Limited Data Set in accordance with the HIPAA Privacy Rule. The Disclosure of a Limited Data Set under this section is subject to the QE's compliance with policies adopted by the QE, which set forth criteria that will be utilized to determine when a proposed Disclosure under this section must be approved by an Institutional Review Board or QE Research Committee.

1.7.3 Research Involving Protected Health Information.

a. Use of Protected Health Information for Patient Recruitment for Research. Affirmative Consent shall not be required for a QE to review Protected Health Information on behalf of a researcher to determine which individuals may qualify for a Research study. In addition, Affirmative Consent shall not be required for a QE to Disclose the name and other identifying information of an individual who may qualify for a Research study to a Participant that has a treating relationship with such individual so that the Participant may contact the individual to determine the individual's willingness to participate in such study, provided that all of the following requirements are met:

i. an Institutional Review Board has approved of such Disclosure;

ii. a QE Research Committee has approved of such Disclosure;

iii. the Data Supplier(s) that are the source of the Protected Health

Information have agreed to allow for the Disclosure of their Protected Health Information for purposes of Research; and

iv. The Disclosure does not include any mental health clinical information governed by Section 33.13 of the Mental Hygiene Law, unless the recipient of the Disclosure is a facility as defined in the Mental Hygiene Law.

b. Use of Protected Health Information for Retrospective Research. Affirmative Consent shall not be required for a QE to Disclose Protected Health Information to a researcher conducting Retrospective Research if:

i. an Institutional Review Board has approved of such Disclosure;

ii. a QE Research Committee has approved of such Disclosure; and

iii. the Data Supplier(s) that are the source of the Protected Health Information have agreed to allow for Disclosures of their Protected Health Information for purposes of Research.

1.7.4 Other Requirements Relating to Research. A QE shall not allow a Participant to opt out of having its Protected Health Information de-identified or converted into a Limited Data Set and used for Research that complies with Section 1.7.1, 1.7.2, or 1.7.5, if applicable.

1.7.5 Research Involving Multiple QEs. If a researcher seeks to obtain information from multiple QEs for purposes of Research, via sPRL or otherwise, then the QEs and the researcher shall comply with the following:

a. The researcher shall present the proposed research to a QE for initial screening. If the QE determines the proposed Research project is appropriate, the proposal shall be submitted to the Centralized Research Committee for approval, in lieu of approval by a QE Research Committee, if (i) the researcher would receive Protected Health Information that does not solely consist of a Limited Data Set, or (ii) the researcher would receive De-Identified Data or a Limited Data Set and the policies adopted by one of the QEs that is the source of such information would require approval by the QE Research Committee of such QE. Notwithstanding the foregoing, if the researcher would obtain information from only two QEs, then approval by the Centralized Research Committee is not necessary if the QE Research Committee of one such QE approves the Research and the other QE consents to such approval.

b. If the Centralized Research Committee approves a Research project, a QE may still decline to provide information requested for such Research project on the basis of costs, lack of resources, or another reason that is unrelated to the merits of the proposed Research.

c. A QE that receives information from another QE for a Research project shall keep such information separate from other information maintained by the

QE. The QE shall ensure that such information is only used for the Research project for which it was obtained and shall delete such information from its systems within a reasonable time period after the Research is completed. Such QE shall have no obligation to correct errors in the information it receives from another QE.

1.8 Transmittals to Non-Participants.

1.8.1 Transmittals to Business Associates. In any case where a Participant has a right to Access or receive Protected Health Information under these Policies and Procedures, the Participant may request that a QE Transmit such information to a Business Associate of the Participant, and the QE may comply with such request, so long as the conditions set forth in subsections (a) through (f) are met. Nothing in this section shall allow a QE to treat a Business Associate as a Participant unless the Business Associate otherwise meets the definition of a Participant.

a. The Participant and the Business Associate have entered into a Business Associate Agreement under which the Business Associate agrees to protect the confidentiality of the Protected Health Information being Transmitted to the Business Associate.

b. The Participant represents to the QE in writing that its Business Associate is seeking the Participant's information in accordance with the terms of the Business Associate Agreement between the two parties.

c. The Business Associate and the Participant agree to provide a copy of their Business Associate Agreement to the QE upon request.

d. The QE reasonably believes that the Transmittal is in accordance with state and federal law and the terms of the Business Associate Agreement.

e. The QE either enters into an agreement with the Business Associate requiring the Business Associate to comply with these Policies and Procedures or the Participation Agreement between the Participant and the QE holds the Participant responsible for the actions of the Business Associate.

f. The Business Associate agrees not to further Disclose the Protected Health Information except where these Policies and Procedures allows for such Disclosure.

1.8.2 Transmittals to Other Non-Participants. A QE may Transmit a patient's Protected Health Information from the QE (or any other QE that has agreed to such Transmittal) to a health care provider or other entity that is not a Participant or a Business Associate of a Participant only if all of the following conditions are met:

a. The patient has granted Affirmative Consent for the Transmittal, provided that Affirmative Consent shall not be required if the Transmittal is provided to a public health authority, as defined at 45 C.F.R. § 164.501. The Affirmative Consent shall meet all the requirements of a Level 1 Consent or Alternative Consent, provided that if the recipient is a life or disability

insurer that is not a governmental entity then the form shall have been approved by the applicable department(s) of insurance. For the avoidance of doubt, (i) a Transmittal may be made to a non-Participant on the basis of any Affirmative Consent that applies to such non-Participant, and (ii) none of the exceptions to the Affirmative Consent requirement set forth in Section 1.2 other than Section 1.2.2 shall apply to Transmittals under this section.

b. The recipient of the Transmittal is not a Participant and is one of the following:

   i. A Covered Entity that does not operate in New York State, or a Business Associate of such Covered Entity.

   ii. A Health Information Exchange Organization that does not operate in New York State.

   iii. A public health authority, as defined at 45. C.F.R. § 164.501, that is not located in New York State.

   iv. A health care facility that is operated by the United States Department of Veteran Affairs or the United States Department of Defense.

   v. A disability insurer or life insurer that has (i.) issued a disability or life insurance policy to the patient; (ii.) received an application from the patient for such a policy; or (iii.) received a claim for benefits from the patient.

c. The QE takes reasonable measures, or requires the recipient to take reasonable measures, to authenticate that the person who has granted the Affirmative Consent is the patient or the patient's Personal Representative.

d. The QE takes reasonable measures to authenticate that the recipient is the same individual or entity authorized in the patient's Affirmative Consent to receive the patient's Protected Health Information.

e. The QE enters into an agreement with the recipient that requires the recipient to:

   i. Obtain the Affirmative Consent of the patient that is the subject of the Protected Health Information, or ensure that another entity or organization has obtained such consent;

   ii. Abide by the terms of patients' Affirmative Consents and applicable law (e.g., health privacy laws for a Covered Entity, insurance laws for life and disability insurers), including any restrictions on re-disclosure;

   iii. Notify the QE in writing and in the most expedient time possible if the recipient becomes aware of any actual or suspected Breach of

Unsecured Protected Health Information;

iv. Represent that the recipient is not excluded, debarred, or otherwise ineligible from participating in any federal health care programs; and

v. Not engage in the sale of the Protected Health Information provided to the recipient, or the use or disclosure of such Protected Health Information for marketing purposes in a manner that would be prohibited by the HIPAA Privacy Rule if such rule were applicable to the recipient, unless the recipient obtains the patient's authorization to do so in a form that complies with the HIPAA Privacy Rule.

Nothing in this section shall be construed to prohibit a patient from Disclosing any of the patient's Protected Health Information the patient has received from a QE under Section 5.2 or 5.3 to an individual or entity of the patient's choice.

1.9 Other Policies and Procedures Related to Consent.

1.9.1 Affiliated Practitioners. An Affirmative Consent that applies to 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 such Affiliated Practitioner's 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.

1.9.2 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.

1.9.3 QEs and Participants may use Affirmative Consents that apply to more than one Participant, subject to the following conditions.

a. The organization offering the multi-Participant consent to the patient must inform the patient that the patient has an option to sign a consent form that applies only to a single Participant. The organization may provide such information verbally, in the text of the consent form itself, or otherwise.

b. If the multi-Participant consent allows a Participant to Access or receive any patient records that are subject to the rules governing federally assisted alcohol or drug abuse programs at 42 C.F.R. Part 2, the consent form must comply with all relevant restrictions in 42 C.F.R. Part 2.

c. An Affirmative Consent may apply to Participants who join the QE after the date the patient signs the consent form, provided that: (i) the QE maintains a list of its Participants on its website and updates that list within 24 hours of when a new Participant is granted Access to patient information via the

SHIN-NY; (ii) the QE mails a hard copy list of its Participants without charge to any patient who requests that list within 5 business days of the request, (iii) the consent form provides patients with information on how they may obtain a list of Participants, and (iv) Access to any patient records that are subject to the rules governing federally-assisted alcohol or drug abuse programs complies with 42 C.F.R. Part 2.

1.9.4 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.

1.9.5 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. See Electronic Signatures and Records Act (State Technology Law Article III, 9 N.Y.C.R.R. Part 540, New York State Office of Information Technology Services ESRA Guidelines NYS-G04-001).

1.9.6 Denial of Consent. A Level 1 or Level 2 Consent shall give the patient the option of granting or affirmatively denying consent for individual Participants to Access or receive information about the patient via the SHIN-NY. A patient's decision not to sign a consent shall not be construed as a "denial of consent" under Section 1.2.4(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 SHIN-NY to Access or receive the patient's information, except as set forth in Section 1.2.2(b) or Section 1.2.8.

1.9.7 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.

1.9.8 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 or received Protected Health Information via the SHIN-NY prior to such revocation and incorporated such Protected Health Information into its records from retaining such information in its records.

1.9.9 Notification of a QE's Data Suppliers. A QE shall provide, or shall require its Participants to provide, patients with a list of or reference to all of the QE's Data Suppliers at the time the QE or Participant obtains the patient's Affirmative Consent. Each QE shall provide an updated list of the QE's Data Suppliers in compliance with Section 5.1.2.

1.9.10 Compliance with Business Associate Agreements with Data Suppliers. A QE shall execute a Business Associate Agreement with each Data Supplier that is a Covered Entity. A QE shall not use or Disclose Protected Health Information in any manner that violates the QE's Business Associate Agreements.

1.9.11 Disclosure to QE 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.

1.9.12 Compliance with Existing Law. All Access to Protected Health Information via the SHIN-NY 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 or receiving 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.

1.9.13 Compliance with Requests for Restrictions on Disclosures to a Payer Organization. QEs shall develop processes to ensure that a Payer Organization does not Access or receive Protected Health Information 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 that satisfies this requirement, a QE shall be deemed to have complied with the requirement if both of the following are met:

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.

b. Upon receipt of an Affirmative Consent covering a Payer Organization, the Payer Organization, QE or other organization that receives such consent notifies the patient in writing that the patient's 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 they do not agree to the revocation of the prior request.

1.9.14 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 or receipt of 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. Such policies shall ensure that the QE, either directly or from one of its Participants, has received an attestation that includes all the elements set forth in 45 C.F.R. § 164.509, to the extent such attestation is required by the HIPAA Privacy Rule. This section applies to Disclosures of Protected Health

Information to Health Oversight Agencies, except that it does not apply to Disclosures of Protected Health Information to Public Health Agencies under Section 1.2.2.

1.9.15 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.

1.9.16 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.

1.10 Patient Consent Transition Rules. QEs and their Participants may continue to use existing Affirmative Consents after the Consent Implementation Date if the existing consent is approved by NYS DOH under Section 1.3.

1.11 Waivers During a Public Health Emergency. NYS DOH may waive provisions in this Section 1 and other provisions of these Policies and Procedures during a public health emergency under Section 319 of the Public Health Services Act if (i) the waiver assists QEs and/or their Participants in their response to the public health emergency; (ii) NYS DOH provides public notice of such waiver; and (iii) the waiver complies with applicable state and federal law.

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. 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. 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. They are designed to limit exchange of information to the minimum number of individuals 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; 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 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. Emergency Access or "Break the Glass" - a (i) Practitioner; (ii) Authorized User acting under the direction of a Practitioner; or (iii) Emergency Medical Technician who, under the provisions of 1.2.4 ('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;

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 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.

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 is who the individual 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. 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. Such authentication shall take place in accordance with the provisions of this Section 3.

3.2 Authentication Requirements. In light of the importance of strong security measures regarding the protection of patient data and authentication standard requirements for exchanges, including but not limited to the New York State Medicaid Program, QEs shall authenticate, and shall require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Authenticator Assurance Level 2 (AAL2) set forth in National Institute of Standards and Technology Special Publication 800-63 (hereinafter, "NIST SP 800-63").

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.

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: (i.) Only Authorized Users and Certified Applications Access information via the SHIN-NY; and (ii.) 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 (i) assigned a unique username and password to provide such Authorized User with Access to patient information via the SHIN-NY or (ii) complies with any other authentication requirements developed through the SCP. 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 the NIST SP 800-63 guidelines, as may be revised periodically.

4.1.3 Group or temporary usernames shall be prohibited.

4.1.4 Authorized Users shall be required to change their passwords in accordance with the NIST SP 800-63 guidelines, as may be revised periodically.

4.1.5 Authorized Users shall be prohibited from sharing their usernames, passwords or other authentication tools (e.g., tokens), with others and from using the usernames, passwords or other authentication tools 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 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 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 (i.) A QE's health information Access policies and procedures are clear; and (ii.) 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. Such training may be tailored to reflect the purposes for which an Authorized User is authorized to Access Protected Health Information through the QE as well as the nature and scope of the Protected Health Information Accessed.

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.

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.

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

4.7.4 QEs shall, or shall require their Participants to, ensure that each Authorized User undergoes continuing and/or refresher training. QEs may determine appropriate intervals for such refresher trainings. QEs may consider factors such as a Participant's history of compliance with these Policies and Procedures in determining the frequency of refresher trainings for some or all of the Participant's Authorized Users. QEs shall ensure that records of such training are maintained and available for audit for a period of at least six years.

4.7.5 QEs shall collaborate with their Participants with the goal of ensuring that the content of any SHIN-NY specific training is not unduly repetitive with other privacy-related trainings provided to Participants. Such trainings shall focus on SHIN-NY specific requirements that exceed the requirements imposed by applicable law, such as the consent requirements in these Policies and Procedures (including minor consent requirements under these Policies and Procedures). Nothing herein shall prohibit QEs or their Participants from combining the content of SHIN-NY trainings with other privacy-focused trainings.

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) is terminated 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.

4.8.2 QEs shall require their Participants to notify the QE (i) immediately or as promptly as reasonably practicable but in any event within one business day of termination of an Authorized User's employment or other affiliation with the Participant, and (ii) as promptly as reasonably practicable following a change in an Authorized User's role with the Participant that renders the Authorized User's continued Access to the QE inappropriate under the role-based Access standards adopted under Section 2.1. The QE shall immediately or as promptly as reasonably practicable but in any event within one business day of the receipt of notification terminate any such Authorized User's Access to the QE.

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.

4.9 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 the individual 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 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 periodically.

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 1.9.1.

SECTION 5: PATIENT EDUCATION, ENGAGEMENT AND ACCESS

Purpose/Principles

The importance of patient engagement in health care is well-recognized and provides a compelling rationale for facilitating a patient's ability to readily access their Protected Health Information. QEs present an opportunity for patients to gain access to their health information in an electronic format. Such access helps to reduce many of the bureaucratic hurdles patients currently endure when attempting to access their Protected Health Information. Openness about policies, procedures, technology, and practices among Participants exchanging health information via the SHIN-NY 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 requirements that 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 Patient Education and Resources.

5.1.1 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 and inform the patients and/or their Personal Representatives of the benefits and risks of providing an Affirmative Consent for their Protected Health Information to be shared through the QE.

5.1.2 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 or their Personal Representatives, as appropriate, with:

a. Notice, in a manner easily understood by patients, that their Protected Health Information is being uploaded to a QE;

b. a complete, accurate and updated list of the QE's Data Suppliers;

c. information about how to contact Data Suppliers;

d. 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 1.9.6;

e. information about how patients can submit requests to correct erroneous data;

f. information about how patients can submit requests for Audit Logs, in compliance with Section 6.4; and

g. information about the security practices of the SHIN-NY, including the right of patients to be notified of certain breaches (as addressed in Section 7.2.2) and how data sent outside the SHIN-NY upon a patient request may no longer be subject to HIPAA.

5.1.3 The materials referenced in Sections 5.1.1. and 5.1.2 shall be made available on each QE's website. In addition, QEs shall make available appropriate materials to their Participants, in either written or electronic form, so such Participants can provide information to their patients about the SHIN-NY and the consent process.

5.2 Patient Access to SHIN-NY Data. QEs shall facilitate the access of patients and their Personal Representatives to patients' Protected Health Information maintained by the QE through one of the mechanisms set forth in Section 5.2. Each patient shall have the right to indicate the scope of the Protected Health Information and which of the mechanisms they prefer to utilize to obtain access to their information, and the QE shall abide by the patient's request unless applicable law (including the patient access provisions under the HIPAA Privacy Rule or the requirements for the "content and manner" exception or another exception to the Information Blocking Rules) permit or require the QE to limit the scope and form of the Protected Health Information provided to the patient. A QE shall only facilitate such access after confirming the identity of the patient or the patient's Personal Representative through adequate identity proofing procedures.

5.2.1 A QE's own web-based portal or Participants' web-based portals.

5.2.2 A web-based portal established by or maintained by a third party on behalf of a patient, including a Patient App, provided the requirements related to disclosures to third parties set forth in Section 5.3 are met.

5.2.3 A paper or electronic copy of information maintained about the patient by the QE.

5.2.4 Any other mechanism requested by the patient (provided that the QE need not provide the Protected Health Information via the requested mechanism if applicable law, including the Information Blocking Rules, permit the QE to use an alternative mechanism).

5.3 Patient Direction to Patient Apps and Other Third Parties. A QE shall have the means of receiving and responding to requests from patients and Personal Representatives to Disclose such patients' Protected Health Information to third parties, including but not limited to Patient Apps, friends and family of patients, and legal representatives of patients. A QE shall abide by the following requirements in response to such requests:

5.3.1 A QE shall Disclose the patient's Protected Health Information in response to the patient's or Personal Representative's request only after confirming the identity of the patient or the patient's Personal Representative that submitted the request through adequate identity proofing procedures. For example, a QE may require patients to provide their demographic information in conjunction with an image of their government-issued photo ID.

5.3.2 A QE shall decline to fulfill the request, or fulfill the request only in part, only if applicable law permits the QE to do so or if the patient or Personal Representative withdraws the request. Applicable law may include, but is not limited to, the patient access provisions under the HIPAA Privacy Rule, the Information Blocking Rules, or state laws that limit disclosures to Patient Apps.

5.3.3 If the third party to receive the patient's Protected Health Information is a Patient App, the QE shall educate the patient or the patient's Personal Representative about the risks of Disclosure to such Patient App prior to making the Disclosure. Such education shall be based on analyses or recommendations of neutral third parties that evaluate Patient Apps, such as the CARIN Alliance, and comply with any guidance issued by NYS DOH and/or the State Designated Entity regarding the nature of such education. If the patient or the patient's Personal Representative does not withdraw the request in response to such information, the QE shall comply with the request unless applicable law permits the QE to decline to fulfill the request in whole or in part.

5.3.4 A QE may require a patient, a patient's Personal Representative, or a third party to pay a fee prior to Disclosing Protected Health Information to a third party only if applicable law, including the patient access provisions under the HIPAA Privacy Rule and the Information Blocking Rule, permit such fee to be charged. For example, if a QE establishes a portal or other internet-based method that allows a patient, a patient's Personal Representative, or third party to Access Protected Health Information, the QE may not charge a fee for use of that system if no manual effort was required by the QE to fulfill the request.

5.4 Information About Minors. Access of patients, their Personal Representatives, their family members, their informal caregivers and their friends to Protected Health Information must be in accordance with laws granting minors the right to keep information regarding Minor Consent Services confidential from their parents or guardians. Notwithstanding Section 5.2 and 5.3, if a QE does not have a practical means of ensuring that information regarding Minor Consent Services be segregated or otherwise filtered from other Protected Health Information about a minor who is between the ages of 10 and 17 and the Information Blocking Rule requirements at 45 C.F.R. § 171.204 are met, then the QE may deny Disclosure of all of such minor's Protected Health Information to that minor's Personal Representatives, family, informal caregivers, and friends.

5.5 Patient Input and Participation. 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 Requests to Correct Erroneous Information.

5.6.1 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.

5.6.2 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.

5.6.3 Each QE shall make reasonable efforts to provide its Participants with information indicating which other QE Participants have Accessed or received erroneous information that the Participant has corrected at the request of patients in accordance with Section 5.6.1.

5.6.4 If the QE determines that the error is due in part due to a QE's data aggregation and exchange activities (instead of solely due to an error in the underlying record maintained by the applicable Participant[s]), then the QE shall comply with Section 6.6.

SECTION 6: AUDIT

Purpose/Principles

Audits are useful oversight tools for recording and examining Access to and receipt of information through a QE (e.g., who Accessed what data and when). Audits are necessary for verifying compliance with Access controls, like those specified in Section 4, and are 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 and receipt of health information via the SHIN-NY.

Policies and Procedures

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

6.1.1 Audit Logs shall, at a minimum, include the following information regarding each instance of Access to Protected Health Information via the SHIN-NY:

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);

g. Unsuccessful Access (log-in) attempts; and

h. Whether Access occurred through a Break the Glass incident.

6.1.2 Audit Logs shall, at a minimum, include the following information regarding each Transmittal of Protected Health Information via the SHIN-NY:

a. The identity of the patient whose Protected Health Information was Transmitted;

b. The identity of the recipient of the Protected Health Information in the case of a Transmittal;

c. The type of Protected Health Information or record Transmitted (e.g., pharmacy data, laboratory data, etc.);

d. The date and time of Transmittal; and

e. The source of the Protected Health Information (i.e., the identity of the Participant from whose records the Transmittal of Protected Health Information was derived).

6.1.3 Other Requirements Regarding Audit Logs and Access.

a. 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.

b. 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 Other Requirements Regarding Audit Logs and Transmittals.

a. A QE shall not be required to include a Transmittal within an Audit Log in cases where a QE Transmits Protected Health Information from one Participant to another Participant, or to a Business Associate of another Participant, in accordance with written instructions from the recipient and without modification to the data being Transmitted (as may occur in the case of a One-to-One Exchange).

b. In the case where a QE performs analytics on behalf of a Participant by running queries on a data set, if a patient's Protected Health Information is returned in response to such query, then such result shall not be considered a Transmittal, and a QE shall not be required to include a record of such query in the patient's Audit Log. If the analytics process results in the production of a data set which is Transmitted by the QE to the Participant and such data set includes Protected Health Information of a patient that is derived from the records of any Data Supplier other than the Participant receiving the data set, the QE shall record such Transmittal in the patient's Audit Log.

6.1.5 General Audit Log Requirements.

a. 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.

b. Audit Logs shall be maintained for a period of at least six years from the date on which information is Disclosed.

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 Disclosed via the SHIN-NY, other than in Break the Glass situations;

b. That Authorized Users who Access Protected Health Information via the SHIN-NY do so for Authorized Purposes; and

c. That applicable requirements were met, as outlined in Section 1.2.4, where Protected Health Information was Disclosed 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 Disclosed via the SHIN-NY:

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 Disclosure; and

c. The type of Protected Health Information or record that was Disclosed (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 their 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 provide patients, upon request, with the following information:

a. The name of each Participant that Accessed or received the patient's Protected Health Information in up to the prior 6-year period;

b. The time and date of the Disclosure(s); and

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

6.4.2 If a patient requests the name(s) of the Authorized User(s) who Accessed the patient's Protected Health Information through a specific Participant in up to the prior 6-year period, the QE and that Participant shall take the following actions:

a. The QE shall inform the Participant of the request and shall provide the Participant with the list of the Participant's Authorized User(s) who Accessed the patient's Protected Health Information through the QE in up to the prior 6-year period.

b. The Participant shall either provide the list of Authorized User(s) to the patient or undertake an audit to determine if the Authorized User(s) on the list appropriately Accessed the patient's Protected Health Information for Authorized Purposes.

c. If the Participant chooses to undertake an audit of its Authorized User Access and determines that all of the Authorized User(s) Accessed the patient's information for Authorized Purposes, the Participant shall inform

the patient of this finding and need not provide the patient with the names of the Authorized User(s) who Accessed that patient's information.

d. If the Participant chooses to undertake an audit of its Authorized User Access and determines that one or more of the Authorized User(s) did not Access the patient's information for Authorized Purposes, the Participant shall (i) inform the patient of this finding; (ii) provide the patient with the name(s) of the Authorized User(s) who inappropriately Accessed the patient's information unless the Participant has a reasonable belief that such disclosure could put the Authorized User at risk of harm, in which case the Participant shall provide the patient with an opportunity to appeal this determination to a representative who is more senior to the individual(s) who made the original determination; and (iii) inform the QE of the inappropriate Access and otherwise comply with the requirements of Section 7.

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.

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 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 or received 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.

SECTION 7: BREACH

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 or Transmitted via the SHIN-NY.

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: 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 that are not Covered Entities, other than a public health authority or a Health Oversight Agency , Accessing Protected Health Information through the SHIN-NY 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, other than a public health authority or a Health Oversight Agency, that receives Protected Health Information shall adopt the administrative, physical and technical safeguards that are required under the HIPAA Security Rule related to such Protected Health Information and shall assess whether addressable safeguards under the HIPAA Security Rule should be adopted. In determining which addressable safeguards to adopt, such Participants shall take into account their size, complexity, capabilities, and other factors set forth under 45 C.F.R. Section 164.306(b). Nothing herein shall be construed to require Participants to comply with the HIPAA Security Rule and the HIPAA Privacy Rule with respect to information that does not constitute Protected Health Information.

8.3 Community-Based Organizations Not Subject to HIPAA. A QE may conduct due diligence in regard to a Community-Based Organization that is not a Covered Entity that is seeking to become the QE's Participant, and may reject such organization's request to become a Participant on the basis that the organization does not have sufficient security protocols or any other reason related to privacy or security, so long as such reason does not constitute illegal discrimination. If a QE recognizes a Community-Based Organization that is not a Covered Entity as a Participant, then the following requirements shall apply, in addition to those set forth in Section 8.2:

8.3.1 A Community-Based Organization that is not a Covered Entity may Access Protected Health Information via the SHIN-NY if the patient has executed an Affirmative Consent that permits Disclosure to such Community-Based Organization and the QE abides by the minimum necessary requirements set forth in Section 8.3.3.

8.3.2 QEs and their Participants may Transmit Protected Health Information to a Community-Based Organization that is not a Covered Entity if the Transmittal occurs via direct or another encrypted means of communication and the following conditions are met:

a. the patient has executed an Affirmative Consent that permits Disclosure to such Community-Based Organization; or

b. the Transmittal meets the requirements of a One-to-One Exchange under Section 1.2.1 or is a Patient Care Alert that meets the requirements of Section 1.2.9, and the Transmittal occurs in compliance with the HIPAA Privacy Rule and any other applicable federal law.

8.3.3 A QE or Participant shall undertake reasonable efforts to limit the Protected Health Information Accessed by or Transmitted to a Community-Based Organization that is not a Covered Entity to the minimum amount necessary to accomplish the intended purpose of the Access or Transmittal, taking into account the nature of the Community-Based Organization Accessing the Protected Health Information or receiving the Transmittal, the reason(s) such organization has requested the Protected Health Information, and other relevant factors.

8.3.4 A Community-Based Organization that is not a Covered Entity may redisclose the Protected Health Information it receives via the SHIN-NY only to (i) the patient or the patient's Personal Representative; and (ii) another Participant for purposes of Treatment or Care Management.

SECTION 9: SANCTIONS

Purpose/Principles

Sanctions are an important mechanism for ensuring that Participants and Authorized Users comply with these Policies and 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:

9.2.1 whether the violation was a first time or repeat offense;

9.2.2 the level of culpability of the Participant or Authorized User, e.g., whether the violation was made intentionally, recklessly or negligently;

9.2.3 whether the violation constitutes a crime under state or federal law; and

9.2.4 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:

9.3.1 requiring an Authorized User to undergo additional training with respect to participation in the QE;

9.3.2 temporarily restricting an Authorized User's Access to the QE;

9.3.3 terminating the Access of an Authorized User to the QE;

9.3.4 suspending or terminating a Participant's participation in the QE; and

9.3.5 the assessment of fines or other monetary penalties.

SECTION 10: CYBERSECURITY

Purpose/Principles

At the very core of these Policies and Procedures is the understanding of the critical need for the SHIN-NY to be highly trusted by all the stakeholders if it is ever to realize its full potential in supporting health care transformation and improvement in New York State.

There are two major elements to this policy. First, protecting the privacy of patient information and second, securing the SHIN-NY Enterprise. While security has always been a part of the guidance provided by these Policies and Procedures, the increasing scope and frequency of security breaches, many involving health information, have given a new sense of urgency to making certain that these Policies and Procedures are aligned with current cybersecurity best practices.

The set of policies and procedures outlined in this Section 10 is aimed at securing the Protected Health Information transmitted via the SHIN-NY Enterprise, managing the risk of exposure or compromise, assuring a secure and stable IT environment, and identifying and responding to events involving information asset misuse, loss or unauthorized disclosure.

In general, the key principles underlying these policies align with the federal NIST Cybersecurity Framework standards that are based on key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk. The NIST Cybersecurity Framework principal core functions include:

- Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Policies and Procedures

10.1 Certification. QEs and the Statewide Data Infrastructure shall be certified by the NYS DOH-approved certification body.

10.2 Role of Statewide CISO. The Statewide CISO shall provide guidance and oversight to QE CISOs in identifying, developing, implementing, and maintaining processes across the SHIN-NY Enterprise to reduce information technology risks. In addition, the Statewide CISO shall coordinate and collaborate with QE CISOs to respond to incidents, establish appropriate standards and controls, manage security technologies and direct the establishment of policies and procedures.

10.3 CSPP. Cybersecurity Policy and Procedures (CSPP) shall be developed to assess, manage and mitigate risks associated with access, use, storage, sharing, and transmission of data and to protect the SHIN-NY Enterprise. The State Designated Entity (SDE) shall develop a CSPP consistent with the requirements of the NYS DOH-approved certification body, and apply it to its own operations and its third-party vendors that provide services to the SDE and SHIN-NY Enterprise. Each QE shall develop a CSPP consistent with the requirements of the NYS DOH-approved certification body, and apply it to its own operations and its third-party vendors that provide services to the QE and the SHIN-NY Enterprise.

10.4 CSPP Content. The CSPP shall include policies and procedures that are consistent with the requirements of the NYS DOH-approved certification body and address the following areas:

10.4.1 Cybersecurity governance and roles and responsibilities that shall include but not be limited to the roles of the CEO, CIO, CISO, legal staff, security staff, information technology staff, human resources staff and other appropriate staff in promoting cybersecurity.

10.4.2 Identify.

a. Asset Management.

i. Development and maintenance of an inventory of information technology assets including physical and virtual software and hardware.

ii. Information classification that identifies appropriate controls to protect critical information assets such as data, records, and files.

b. Risk Management that shall include but not be limited to:

i. Risk assessment methodology.

ii. Risk assessment responsibilities.

iii. Risk assessment frequency.

iv. Risk remediation strategy.

v. Vendor and supply chain risk management.

10.4.3 Protect.

a. Change control and configuration management.

b. Vulnerability management.

c. Access control management.

d. Identity and authentication management.

e. Network, system and application security.

f. Life cycle management.

g. Patch management.

h. Back up process.

i. Physical security.

j. Data protection (at rest and in transit) and data handling and disposal.

k. Hardware disposal.

l. Personnel security.

m. Acceptable use to address issues that shall include but not be limited to personal use of the SHIN-NY Enterprise, BYOD (Bring Your Own Device), shared accounts, and other activities that are acceptable or prohibited in the SHIN-NY Enterprise.

n. Training and awareness.

o. Audits to include self-assessments and third-party assessments.

10.4.4 Detect.

a. Monitoring and log analysis.

b. Vulnerability assessment.

c. Penetration tests.

d. Incident warning, advisory, and alerts.

10.4.5 Respond.

a. Incident response.

b. Incident analysis, mitigation and improvement.

c. Exercise and training.

d. Communication.

e. Reporting of major successful and suspected intrusions or cyberattacks that shall include but not be limited to:

i. Chain of reporting requirements including internal through escalation to NYS DOH and the Statewide CISO.

ii. Timeframe for reporting events.

iii. Description of the events.

iv. Damage or impact, if known.

10.4.6 Recover.

a. Disaster recovery.

b. Improvement.

c. Communication.

10.4.7 Policy approval and maintenance to include:

a. Annual review and updates of CSPP.

b. Roles of persons responsible for making updates.

c. Process of approval by CEO and CIO on all CSPP updates.

10.5 CSPP review. Each QE, and the SDE, shall conduct an annual review of its respective CSPP as directed by NYS DOH and prescribed by the statewide CISO.

10.6 Cybersecurity insurance. Each QE shall maintain cybersecurity insurance at the level specified in the QEPA.

APPENDIX A: MODEL LEVEL 1 CONSENT

Attachment A-1 Consent Form for Participants Without Emergency Services
Attachment A-2 Consent Form for Participants With Emergency Services

APPENDIX B: MODEL LEVEL 2 CONSENT

Attachment B-1 Payer Consent Form for Payment
Attachment B-2 Research Consent Form
Attachment B-3 Supplemental Security Income (SSI) Application Consent Form

Appendix A
Attachment A-1

New York State Department of Health

Authorization for Access to Patient Information Through a Health Information Exchange Organization

Patient Name	Date of Birth	Patient Identification Number
Patient Address		

I request that health information regarding my care and treatment be accessed as set forth on this form. I can choose whether or not to allow [Name of Provider Organization or Health Plan; or reference to a list of specific Provider Organizations and/or Plans attached to this form] to obtain access to my medical records through the health information exchange organization called [Name of Qualified Entity]. If I give consent, my medical records from different places where I get health care can be accessed using a statewide computer network. [Name of Qualified Entity] is a not-for-profit organization that shares information about people's health electronically and meets the privacy and security standards of HIPAA and New York State Law. To learn more visit [Name of Qualified Entity]'s website at _____.

The choice I make in this form will NOT affect my ability to get medical care. The choice I make in this form does NOT allow health insurers to have access to my information for the purpose of deciding whether to provide me with health insurance coverage or pay my medical bills.

My Consent Choice. ONE box is checked to the left of my choice.
I can fill out this form now or in the future.
I can also change my decision at any time by completing a new form.

☐ **1. I GIVE CONSENT** for [Name of Provider Organization or Health Plan; or reference to a list of specific Provider Organizations and/or Plans attached to this form] to access ALL of my electronic health information through [Name of Qualified Entity] to provide health care.

☐ **2. I DENY CONSENT** for [Name of Provider Organization or Health Plan; or reference to a list of specific Provider Organizations and/or Plans attached to this form] to access my electronic health information through [Name of Qualified Entity] for any purpose.

If I want to deny consent for all Provider Organizations and Health Plans participating in [Name of Qualified Entity] to access my electronic health information through [Name of Qualified Entity], I may do so by visiting [Name of Qualified Entity]'s website at _____ or calling [Name of Qualified Entity] at [insert phone number].

[To be used only if the form is a community-wide consent form:] I understand that upon my request, [Name of Qualified Entity] is required to provide me with a list of all individuals and organizations who have received my electronic health information under the terms of this form.

My questions about this form have been answered and I have been provided a copy of this form.

Signature of Patient or Patient's Legal Representative	Date
Print Name of Legal Representative (if applicable)	Relationship of Legal Representative to Patient (if applicable)

Details about the information accessed through [Name of Qualified Entity] and the consent process:

1. **How Your Information May be Used**. Your electronic health information will be used **only** for the following healthcare services:
   - **Treatment Services.** Provide you with medical treatment and related services.
   - **Insurance Eligibility Verification.** Check whether you have health insurance and what it covers.
   - **Care Management Activities.** These include assisting you in obtaining appropriate medical care, improving the quality of services provided to you, coordinating the provision of multiple health care services provided to you, or supporting you in following a plan of medical care.
   - **Quality Improvement Activities.** Evaluate and improve the quality of medical care provided to you and all patients.

2. **What Types of Information about You Are Included**. If you give consent, the Provider Organization(s) and/or Health Plan(s) listed may access ALL of your electronic health information available through Qualified Entity. This includes information created before and after the date this form is signed. Your health records may include a history of illnesses or injuries you have had (like diabetes or a broken bone), test results (like X-rays or blood tests), and lists of medicines you have taken. This information may include sensitive health conditions, including but not limited to:
   - Alcohol or drug use problems
   - Birth control and abortion (family planning)
   - Genetic (inherited) diseases or tests
   - HIV/AIDS
   - Mental health conditions
   - Sexually transmitted diseases

   If you have received alcohol or drug abuse care, your record may include information related to your alcohol or drug abuse diagnoses, medications and dosages, lab tests, allergies, substance use history, trauma history, hospital discharges, employment, living situation and social supports, and health insurance claims history.

3. **Where Health Information About You Comes From**. Information about you comes from places that have provided you with medical care or health insurance. These may include hospitals, physicians, pharmacies, clinical laboratories, health insurers, the Medicaid program, and other organizations that exchange health information electronically. A complete, current list is available from [Provider Organization(s) *OR Qualified Entity, as applicable].* You can obtain an updated list at any time by checking [Name of Qualified Entity]'s website at _____ or by calling _____].

4. **Who May Access Information About You, If You Give Consent.** Only doctors and other staff members of the Organization(s) you have given consent to access who carry out activities permitted by this form as described above in paragraph one.

5. **Public Health and Organ Procurement Organization Access**. Federal, state or local public health agencies and certain organ procurement organizations are authorized by law to access health information without a patient's consent for certain public health and organ transplant purposes. These entities may access your information through [name of Qualified Entity] for these purposes without regard to whether you give consent, deny consent or do not fill out a consent form.

6. **Penalties for Improper Access to or Use of Your Information.** There are penalties for inappropriate access to or use of your electronic health information. If at any time you suspect that someone who should not have seen or gotten access to information about you has done so, call the Provider Organization at: _____; or visit [Name of Qualified Entity]'s website: _____; or call the NYS Department of Health at 518-474-4987; or follow the complaint process of the federal Office for Civil Rights at the following link: *http://www.hhs.gov/ocr/privacy/hipaa/complaints/.*

7. **Re-disclosure of Information.** Any organization(s) you have given consent to access health information about you may re- disclose your health information, but only to the extent permitted by state and federal laws and regulations. Alcohol/drug treatment- related information or confidential HIV-related information may only be accessed and may only be re-disclosed if accompanied by the required statements regarding prohibition of re-disclosure.

8. **Effective Period**. This Consent Form will remain in effect until the day you change your consent choice or until such time as Qualified Entity ceases operation ***(or until 50 years after your death whichever occurs first)***. If Qualified Entity merges with another Qualified Entity your consent choices will remain effective with the newly merged entity.

9. **Changing Your Consent Choice**. You can change your consent choice at any time and for any Provider Organization or Health Plan by submitting a new Consent Form with your new choice(s). Organizations that access your health information through [Name of Qualified Entity] while your consent is in effect may copy or include your information in their own medical records. Even if you later decide to change your consent decision, they are not required to return your information or remove it from their records.

10. **Copy of Form**. You are entitled to get a copy of this Consent Form**.**

Appendix A
Attachment A-2

New York State Department of Health

Authorization for Access to Patient Information Through a Health Information Exchange Organization

Patient Name	Date of Birth	Patient Identification Number
Patient Address		

I request that health information regarding my care and treatment be accessed as set forth on this form. I can choose whether or not to allow [Name of Provider Organization or Health Plan; or reference to a list of specific Provider Organizations and/or Plans attached to this form] to obtain access to my medical records through the health information exchange organization called [Name of Qualified Entity]. If I give consent, my medical records from different places where I get health care can be accessed using a statewide computer network. [Name of Qualified Entity] is a not-for-profit organization that shares information about people's health electronically and meets the privacy and security standards of HIPAA and New York State Law. To learn more visit [Name of Qualified Entity]'s website at _____.

My information may be accessed in the event of an emergency, unless I complete this form and check box #3, which states that I deny consent *even* in a medical emergency.

The choice I make in this form will NOT affect my ability to get medical care. The choice I make in this form does NOT allow health insurers to have access to my information for the purpose of deciding whether to provide me with health insurance coverage or pay my medical bills.

My Consent Choice. ONE box is checked to the left of my choice.
I can fill out this form now or in the future.
I can also change my decision at any time by completing a new form.

☐ **1. I GIVE CONSENT** for [Name of Provider Organization or Health Plan; or reference to a list of specific Provider Organizations and/or Plans attached to this form] to access ALL of my electronic health information through [Name of Qualified Entity] to provide health care services (including emergency care).

☐ **2. I DENY CONSENT EXCEPT IN A MEDICAL EMERGENCY** for [Name of Provider Organization or Health Plan; or reference to a list of specific Provider Organizations and/or Plans attached to this form] to access my electronic health information through [Name of Qualified Entity].

☐ **3. I DENY CONSENT** for [Name of Provider Organization or Health Plan; or reference to a list of specific Provider Organizations and/or Plans attached to this form] to access my electronic health information through [Name of Qualified Entity] for any purpose, ***even*** *in a medical emergency*.

If I want to deny consent for all Provider Organizations and Health Plans participating in [Name of Qualified Entity] to access my electronic health information through [Name of Qualified Entity], I may do so by visiting [Name of Qualified Entity]'s website at _____ or calling [Name of Qualified Entity] at [insert phone number].

[To be used only if the form is a community-wide consent form:] I understand that upon my request, [Name of Qualified Entity] is required to provide me with a list of all individuals and organizations who have received my electronic health information under the terms of this form.

My questions about this form have been answered and I have been provided a copy of this form.

Signature of Patient or Patient's Legal Representative	Date
Print Name of Legal Representative (if applicable)	Relationship of Legal Representative to Patient (if applicable)

Details about the information accessed through [Name of Qualified Entity] and the consent process:

1. **How Your Information May be Used**. Your electronic health information will be used **only** for the following healthcare services:
   - **Treatment Services.** Provide you with medical treatment and related services.
   - **Insurance Eligibility Verification.** Check whether you have health insurance and what it covers.
   - **Care Management Activities.** These include assisting you in obtaining appropriate medical care, improving the quality of services provided to you, coordinating the provision of multiple health care services provided to you, or supporting you in following a plan of medical care.
   - **Quality Improvement Activities.** Evaluate and improve the quality of medical care provided to you and all patients.

2. **What Types of Information about You Are Included**. If you give consent, the Provider Organization(s) and/or Health Plan(s) listed may access ALL of your electronic health information available through Qualified Entity. This includes information created before and after the date this form is signed. Your health records may include a history of illnesses or injuries you have had (like diabetes or a broken bone), test results (like X-rays or blood tests), and lists of medicines you have taken. This information may include sensitive health conditions, including but not limited to:
   - Alcohol or drug use problems
   - Birth control and abortion (family planning)
   - Genetic (inherited) diseases or tests
   - HIV/AIDS
   - Mental health conditions
   - Sexually transmitted diseases

   If you have received alcohol or drug abuse care, your record may include information related to your alcohol or drug abuse diagnoses, medications and dosages, lab tests, allergies, substance use history, trauma history, hospital discharges, employment, living situation and social supports, and health insurance claims history.

3. **Where Health Information About You Comes From**. Information about you comes from places that have provided you with medical care or health insurance. These may include hospitals, physicians, pharmacies, clinical laboratories, health insurers, the Medicaid program, and other organizations that exchange health information electronically. A complete, current list is available from [Provider Organization(s) *OR Qualified Entity, as applicable].* You can obtain an updated list at any time by checking [Name of Qualified Entity]'s website at _____ or by calling _____].

4. **Who May Access Information About You, If You Give Consent.** Only doctors and other staff members of the Organization(s) you have given consent to access who carry out activities permitted by this form as described above in paragraph one.

5. **Public Health and Organ Procurement Organization Access**. Federal, state or local public health agencies and certain organ procurement organizations are authorized by law to access health information without a patient's consent for certain public health and organ transplant purposes. These entities may access your information through [name of Qualified Entity] for these purposes without regard to whether you give consent, deny consent or do not fill out a consent form.

6. **Penalties for Improper Access to or Use of Your Information.** There are penalties for inappropriate access to or use of your electronic health information. If at any time you suspect that someone who should not have seen or gotten access to information about you has done so, call the Provider Organization at: _____; or visit [Name of Qualified Entity]'s website: _____; or call the NYS Department of Health at 518-474-4987; or follow the complaint process of the federal Office for Civil Rights at the following link: *http://www.hhs.gov/ocr/privacy/hipaa/complaints/.*

7. **Re-disclosure of Information.** Any organization(s) you have given consent to access health information about you may re- disclose your health information, but only to the extent permitted by state and federal laws and regulations. Alcohol/drug treatment- related information or confidential HIV-related information may only be accessed and may only be re-disclosed if accompanied by the required statements regarding prohibition of re-disclosure.

8. **Effective Period**. This Consent Form will remain in effect until the day you change your consent choice or until such time as Qualified Entity ceases operation ***(or until 50 years after your death whichever occurs first)***. If Qualified Entity merges with another Qualified Entity your consent choices will remain effective with the newly merged entity.

9. **Changing Your Consent Choice**. You can change your consent choice at any time and for any Provider Organization or Health Plan by submitting a new Consent Form with your new choice(s). Organizations that access your health information through [Name of Qualified Entity] while your consent is in effect may copy or include your information in their own medical records. Even if you later decide to change your consent decision, they are not required to return your information or remove it from their records.

10. **Copy of Form**. You are entitled to get a copy of this Consent Form after you sign it.

Appendix B
Attachment B-1

MODEL LEVEL 2 PAYER CONSENT FORM FOR PAYMENT
[NAME OF PAYER ORGANIZATION]

In this Consent Form, you can choose whether to allow [Name of Payer Organization] to obtain access to your medical records through a computer network operated by [Name of Qualified Entity], which is part of a statewide computer network. This can help collect the medical records you have in different places where you get health care, and make them available electronically to [Name of Payer Organization].

You may use this Consent Form to decide whether or not to allow [Name of Payer Organization] to see and obtain access to your electronic health records in this way. You can give consent or deny consent, and this form may be filled out now or at a later date.

If you check the **"I GIVE CONSENT"** box below, you are saying "Yes, [Name of Payer Organization] may see and get access to all of my medical records through [Name of Qualified Entity] for the purpose of determining whether to make payment for health care services provided to me."

If you check the **"I DENY CONSENT"** box below, you are saying "No, [Name of Payer Organization] may not be given access to my medical records through [Name of Qualified Entity] for the purpose of determining whether to make payment for health care services provided to me."

[Name of Qualified Entity] is a not-for-profit organization. It shares information about people's health electronically and securely to improve the quality of health care services. This kind of sharing is called ehealth or health information technology (health IT).

Please carefully read the information on the back of this form before making your decision.

Your Consent Choices. You can fill out this form now or in the future. You have two choices.

- ☐ **I GIVE CONSENT for [Name of Payer Organization] to access ALL of** my electronic health information through [Name of Qualified Entity] for the purpose of determining whether to make payment for health care services provided to me.
- ☐ **I DENY CONSENT for [Name of Payer Organization] to access** my electronic health information through [Name of Qualified Entity] for the purpose of determining whether to make payment for health care services provided to me.

_____	_____
Print Name of Patient	Patient Date of Birth
_____	_____
Signature of Patient or Patient's Legal Representative	Date
_____	_____
Print Name of Legal Representative (if applicable)	Relationship of Legal Representative to Patient (if applicable)

Details about patient information in [Name of Qualified Entity] and the consent process:

1. **How Your Information Will Be Used.** Your electronic health information will be used by [Name of Payer Organization] only for the purpose of determining whether to make payment for health care services provided to you. This may include, among other things, determining whether health care services are covered by your insurance, are medically necessary, or are covered by another insurance plan. Your information will not be used for employment-related purposes.

2. **What Types of Information about You Are Included**. If you give consent, [Name of Payer Organization] may access ALL of your electronic health information available through the Qualified Entity. This includes information created before and after the date of this Consent Form and may include information relating to services that were not covered by [Name of Payer Organization]. Your health records may include a history of illnesses or injuries you have had (like diabetes or a broken bone), test results (like X-rays or blood tests), and lists of medicines you have taken. This information may relate to sensitive health conditions, including but not limited to:
   - Alcohol or drug use problems
   - Birth control and abortion (family planning)
   - Genetic (inherited) diseases or tests
   - HIV/AIDS
   - Mental health conditions
   - Sexually transmitted diseases

   If you have received alcohol or drug abuse care, your record may include information related to your alcohol or drug abuse diagnoses, medications and dosages, lab tests, allergies, substance use history, trauma history, hospital discharges, employment, living situation and social supports, and health insurance claims history.

3. **Where Health Information About You Comes From**. Information about you comes from places that have provided you with medical care or health insurance ("Information Sources"). These may include hospitals, physicians, pharmacies, clinical laboratories, health insurers, the Medicaid program, and other ehealth organizations that exchange health information electronically. A complete list of current Information Sources is available from [Name of Payer Organization or Qualified Entity as applicable]. You can obtain an updated list of Information Sources at any time by checking the [Name of Qualified Entity]'s website at _____ or by calling ____.

4. **Who May Access Information About You, If You Give Consent.** Only staff of [Name of Payer Organization] who are involved in the activities for which you have agreed to provide your information may access your information.

5. **Penalties for Improper Access to or Use of Your Information.** There are penalties for inappropriate access to or use of your electronic health information. If at any time you suspect that someone who should not have seen or gotten access to information about you has done so, call [Name of Payer Organization] at: _____; or visit [Name of Qualified Entity]'s website: _____.

6. **Re-disclosure of Information.** Any electronic health information about you may be re-disclosed by [Name of Payer Organization] to others only to the extent permitted by state and federal laws and regulations. This is also true for health information about you that exists in a paper form. Some state and federal laws provide special protections for some kinds of sensitive health information, including HIV/AIDS and drug and alcohol treatment. Their special requirements must be followed whenever people receive these kinds of sensitive health information. [Name of Qualified Entity] and persons who access this information through the [Name of Qualified Entity] must comply with these requirements.

7. **Effective Period**. This Consent Form will remain in effect for two years from the date that you sign this form or until the day you withdraw your consent.

8. **Withdrawing Your Consent**. You can withdraw your consent at any time by signing a Withdrawal of Consent Form and giving it to [Payer Organization or Qualified Entity, as applicable]. You can also change your consent choices by signing a new Consent Form at any time. You can get these forms on [Name of Qualified Entity]'s website at _____, or by calling _____. **Note: Organizations that access your health information through [Name of Qualified Entity] while your consent is in effect may copy or include your information in their own medical records. Even if you later decide to withdraw your consent, they are not required to return it or remove it from their records.**

9. **Copy of Form**. You are entitled to get a copy of this Consent Form after you sign it.

MODEL LEVEL 2 RESEARCH CONSENT FORM
[NAME OF PROVIDER ORGANIZATION]

In this Consent Form, you can choose whether to allow researchers working with [Name of Provider Organization] to obtain access to your medical records for research purposes through a computer network operated by [Name of Qualified Entity], which is part of a statewide computer network. This can help collect the medical records you have in different places where you get health care and make them available electronically to these researchers. This Consent Form should read together with the [Name of Informed Consent For Research Document] you signed when you agreed to participate in one or more research studies.

You may use this Consent Form to decide whether or not to allow researchers working with [Name of Provider Organization] to see and obtain access to your electronic health records in this way. **Your choice will not affect your ability to get medical care or health insurance coverage. Your choice to give or to deny consent may not be the basis for denial of health services[, except that, if you choose to deny consent you will not be eligible to participate in _____].**

If you check the **"I GIVE CONSENT"** box below, you are saying "Yes, [Name of Provider Organization's] researchers may see and get access to all of my medical records through [Name of Qualified Entity] for the research activities described in Section 1 of this Consent Form."

[Name of Qualified Entity] is a not-for-profit organization. It shares information about people's health electronically and securely to improve the quality of health care services. This kind of sharing is called ehealth or health information technology (health IT).

Please carefully read the information on the back of this form before making your decision.

☐ **I GIVE CONSENT for [Name of Provider Organization's] researchers to access** my electronic health information through [Name of Qualified Entity] for the research activities described in Section 1 of this Consent Form.

_____ Print Name of Patient	_____ Patient Date of Birth
_____ Signature of Patient or Patient's Legal Representative	_____ Date
_____ Print Name of Legal Representative (if applicable)	_____ Relationship of Legal Representative to Patient (if applicable)

Details about patient information in [Name of Qualified Entity] and the consent process:

1. **How Your Information Will Be Used.** Your electronic health information will be used by [Name of Provider Organization's] researchers to conduct the following research studies: [Insert Name and Description of Research Studies]. Additional information about these studies is provided in the [reference informed consent document]

2. **What Types of Information about You Are Included.** If you give consent, [Name of Provider Organization's] researchers may access the following types of electronic health information through [Name of Qualified Entity] for research purposes. This includes information created before and after the date of this Consent Form. [Name of Provider Organization's] researchers will only be permitted to use health information that is necessary for the research studies you have agreed to participate in. However, while locating this information and copying it into its own research database, [Name of Provider Organization's] researchers may gain incidental access to ALL of your electronic health information available through the [Name of Qualified Entity]. This information may relate to sensitive health conditions, including but not limited to:
   - Alcohol or drug use problems
   - Birth control and abortion (family planning)
   - Genetic (inherited) diseases or tests
   - HIV/AIDS
   - Mental health conditions
   - Sexually transmitted diseases

   If you have received alcohol or drug abuse care, your record may include information related to your alcohol or drug abuse diagnoses, medications and dosages, lab tests, allergies, substance use history, trauma history, hospital discharges, employment, living situation and social supports, and health insurance claims history.

   [Name of Provider Organization] will take reasonable steps to minimize any incidental access to your health information that is not required for the research studies.

3. **Where Health Information About You Comes From**. Information about you comes from places that have provided you with medical care or health insurance ("Information Sources"). These may include hospitals, physicians, pharmacies, clinical laboratories, health insurers, the Medicaid program, and other ehealth organizations that exchange health information electronically. A complete list of current Information Sources is available from [*Provider Organization OR* Qualified Entity*, as applicable].* You can obtain an updated list of Information Sources at any time by checking the [Name of Qualified Entity]'s website at _____ or by calling _____.

4. **Who May Access Information About You, If You Give Consent.** Only research staff employed by [Provider Organization] or outside researchers working at [Name of Provider Organization] who are involved in the research activities for which you have agreed to provide your information may access your information.

5. **Penalties for Improper Access to or Use of Your Information.** There are penalties for inappropriate access to or use of your electronic health information. If at any time you suspect that someone who should not have seen or gotten access to information about you has done so, call [Name of Provider Organization] at: _____; or visit [Name of Qualified Entity]'s website: _____.

6. **Re-disclosure of Information.** Any electronic health information about you may be re-disclosed by [Name of Provider Organization] to others only to the extent permitted by state and federal laws and regulations. This is also true for health information about you that exists in a paper form. Some state and federal laws provide special protections for some kinds of sensitive health information, including HIV/AIDS and drug and alcohol treatment. Their special requirements must be followed whenever people receive these kinds of sensitive health information. [Name of Qualified Entity] and persons who access this information through the [Name of Qualified Entity] must comply with these requirements. You will not be identified in the published results of any research studies conducted with your information.

7. **Effective Period**. This Consent Form will remain in effect until _____ or the day you withdraw your consent.

8. **Withdrawing Your Consent**. You can withdraw your consent at any time by signing a Withdrawal of Consent Form and giving it to any of the researchers who are overseeing your medical care or [*Provider Organization or* Qualified Entity*, as applicable].* You can get this form from any of [Name of Provider Organization's] researchers or on [Name of Qualified Entity]'s website at _____, or by calling _____.. **Note: If [Name of Provider Organization's] researchers access your health information through [Name of Qualified Entity] while your consent is in effect, they may copy or include your information in their own research databases. Even if you later decide to withdraw your consent, [Name of Provider Organization's] researchers are not required to return your health information or remove it from these databases to the extent maintaining the information is necessary to complete the research study.**

9. **Copy of Form**. You are entitled to get a copy of this Consent Form after you sign it**.**

Appendix B
Attachment B-3

MODEL LEVEL 2 SUPPLEMENTAL SECURITY INCOME (SSI) APPLICATION CONSENT FORM
[NAME OF PROVIDER ORGANIZATION]

In this Consent Form, you can choose whether to allow [Name of Provider Organization] to obtain access to your medical records through a computer network operated by [Name of Qualified Entity], which is part of a statewide computer network, for the purpose of assisting you with your Supplemental Security Income (SSI) application.

In order for the Social Security Administration to make a decision on your eligibility for SSI due to your disability, it is helpful for the application to include:

- medical reports
- names, addresses, and telephone numbers of doctors and other providers of medical services to you and dates that you were treated
- names of prescription and non-prescription medications that you take

You may use this Consent Form to decide whether or not to give [Name of Provider Organization] the right to access your electronic health records to obtain this information, if available, in order to assist you with your SSI application. **Your choice will not affect your ability to get medical care or health insurance coverage. Your choice to give or to deny consent may not be the basis for denial of health services.**

If you check the **"I GIVE CONSENT"** box below, you are saying "Yes, [Name of Provider Organization] may, even though they may not provide treatment to me, see and get access to all of my medical records through [Name of Qualified Entity] for the purpose of assisting me with my SSI application."

[Name of Qualified Entity] is a not-for-profit organization. It shares information about people's health electronically and securely to improve the quality of health care services. This kind of sharing is called ehealth or health information exchange. To learn more about ehealth in New York State, visit the website of the NY eHealth Collaborative at www.nyehealth.org/shin-ny/what-is-the-shin-ny.

Please carefully read the information on the back of this form before making your decision.

☐ **I GIVE CONSENT for [Name of Provider Organization] to access** my electronic health information through [Name of Qualified Entity] for the purposes of assisting me with my SSI application.

Print Your Name	Your Date of Birth
Your Signature or Signature of Your Legal Representative	Date of Signature
Print Name of Legal Representative (if applicable)	Relationship of Legal Representative to You (if applicable)

Details about patient information in [Name of Qualified Entity] and the consent process:

1. **How Your Information Will Be Used.** Your electronic health information will be used by [Name of Provider Organization] to assist you with your application for Supplemental Security Income. If you give consent, [Name of Provider Organization] may access your electronic health information only for this purpose.

2. **What Types of Information about You Are Included.** If you give consent, [Name of Provider Organization] may access the following types of electronic health information through [Name of Qualified Entity]. This includes information created before and after the date the date this form is signed. Your health records may include a history of illnesses or injuries you have had (like diabetes or a broken bone), test results (like X-rays or blood tests), and lists of medicines you have taken. This information may relate to sensitive health conditions, including but not limited to:

- Alcohol or drug use problems
- Birth control and abortion (family planning)
- Genetic (inherited) diseases or tests
- HIV/AIDS
- Mental health conditions
- Sexually transmitted diseases

If you have received alcohol or drug abuse care, your record may include information related to your alcohol or drug abuse diagnoses, medications and dosages, lab tests, allergies, substance use history, trauma history, hospital discharges, employment, living situation and social supports, and health insurance claims history.

3. **Where Health Information About You Comes From**. Information about you comes from places that have provided you with medical care or health insurance ("Information Sources"). These may include hospitals, physicians, pharmacies, clinical laboratories, health insurers, the Medicaid program, and other ehealth organizations that exchange health information electronically. A complete list of current Information Sources is available from [*Name of Provider Organization OR Name of Qualified Entity, as applicable].* You can obtain an updated list of Information Sources at any time by checking [Name of Qualified Entity]'s website at _____ or by calling _____.

4. **Who May Access Information About You, If You Give Consent.** By signing this form, you are allowing staff of members of [Name of Provider Organization] to access your information.

5. **Penalties for Improper Access to or Use of Your Information.** There are penalties for inappropriate access to or use of your electronic health information. If at any time you suspect that someone who should not have seen or gotten access to information about you has done so, call [Name of Provider Organization] at: _____; or visit [Name of Qualified Entity]'s website _____.

6. **Re-disclosure of Information.** Any electronic health information about you may be re-disclosed by [Name of Provider Organization] to others only to the extent permitted by state and federal laws and regulations. This is also true for health information about you that exists in a paper form. Some state and federal laws provide special protections for some kinds of sensitive health information, including HIV/AIDS and drug and alcohol treatment.

7. **Effective Period**. Unless you specify otherwise, this Consent Form will remain in effect for 90 days after the date on which you sign the form or until you withdraw consent. If you would like the form to be in effect for a period of time other than 90 days, please indicate the date on which you would like this Consent Form to expire here: _____. **Note: If [Name of Provider Organization] accesses your health information through [Name of Qualified Entity] while your consent is in effect, it may copy or include your information in its own medical records. Once the effective period expires, [Name of Provider Organization] is not required to return your health information or remove it from its records.**

8. **Withdrawing Your Consent**. You can withdraw your consent at any time by submitting a written request to withdraw that consent, or by calling _____.

9. **Copy of Form**. You are entitled to get a copy of this Consent Form after you sign it**.**