

**Privacy and Security Policies and
Procedures for Qualified Entities and
their Participants in New York State
under 10 NYCRR § 300.3(b)(1)**

Version 3.3

REVISED March 2016

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

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 NYCRR § 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 (“NYSDOH”), 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. NYSDOH 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 NYSDOH’s website.

Target Audience. Qualified Entities (“QEs”) and their participants 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:

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

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

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

Affirmative Consent means the consent of a patient obtained through the patient’s execution of (i) a Level 1 Consent; (ii) a Level 2 Consent; (iii) a consent mechanism approved by NYSDOH as an alternative to a Level 1 Consent or a Level 2 Consent under Section 1.3; or (iv) a consent that may be relied upon under the Patient Consent Transition Rules set forth in Section 1.9.2.

Approved Consent means an Affirmative Consent other than a consent relied upon by a Participant under the Patient Consent Transition Rules set forth in Section 1.9.2.

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

Authorized User means an individual who has been authorized by a Participant or a QE to access patient information via the SHIN-NY governed by a QE in accordance with 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 CFR § 164.504(e).

Care Management means (i) assisting a patient in obtaining appropriate medical care, (ii) improving the quality of health care services provided to a patient, (iii) coordinating the provision of multiple health care services to a patient or (iv) supporting a patient in following a plan of medical care. Care Management does not include utilization review or other activities carried out by a Payer Organization to determine whether coverage should be extended or payment should be made for a health care service.

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

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

Covered Entity has the meaning ascribed to this term in 45 C.F.R. § 160.103 and is thereby bound to comply with the HIPAA Privacy Rule and HIPAA Security Rule.

Data Supplier means an individual or entity that supplies Protected Health Information to or through a QE. Data Suppliers include both Participants and entities that supply but do not access Protected Health Information via the SHIN-NY governed by a QE (such as clinical laboratories and pharmacies).

De-Identified Data means data that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Data may be considered de-identified only if it satisfies the requirements of 45 C.F.R. § 164.514(b).

Demographic Information means a patient's name, gender, address, date of birth, social security number, and other personally identifiable information, but shall not include any information regarding a

patient's health or medical treatment or the names of any Data Suppliers that maintain medical records about such patient.

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.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

Limited Data Set has the meaning ascribed to this term under the HIPAA Privacy Rule.

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

Minor Consent Information means Protected Health Information relating to medical treatment of a minor for which the minor provided his or her own consent without a parent's or guardian's permission, as permitted by New York law or other applicable laws for certain types of health services (e.g., reproductive health, HIV testing, STD, mental health or substance abuse treatment) or services consented to by an Emancipated Minor.

NYSDOH means the New York State Department of Health.

One-to-One Exchange means a disclosure of Protected Health Information by one of the patient's providers or other Participants to one or more other Participants either treating the patient or performing Quality Improvement and/or Care Management activities for such patient with the patient's knowledge and implicit or explicit consent where no records other than those of the Participants jointly providing health care services to the patient are exchanged. A One-to-One Exchange is an electronic transfer of information that is understood and predictable to a patient, because it mirrors a paper-based exchange, such as a referral to a specialist, a discharge summary sent to where the patient is transferred, lab results sent to the Practitioner who ordered them or clinical information sent from a Participant to the patient's health plan for Quality Improvement or Care Management/coordination activities for such patient.

Organ Procurement Organization (OPO) means a regional, non-profit organization responsible for coordinating organ and tissue donations at a hospital that is designated by the Secretary of Health and Human Services under section 1138(b) of the Social Security Act (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, PPS Partner, PPS Centralized 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 governed by a QE.

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

Patient Care Alert means an electronic message about a development in a patient's medical care, such as an emergency room or inpatient hospital admission or discharge, a scheduled outpatient surgery or other procedure, or similar event, which is derived from information maintained by a QE and is sent by the QE to subscribing recipients but does not allow the recipient to access any Protected Health Information through the QE other than the information contained in the message.

Patient Consent Transition Rules means the rules set forth in Section 1.81.9.

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 ERISA or any other entity that is legally authorized to provide health insurance

coverage.

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

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

PPS means a Performing Provider System that has received approval from NYSDOH to implement projects and receive funds under New York's Delivery System Reform Incentive Payment Program.

PPS Partner means a person or entity that is listed as a PPS Partner in the DSRIP Network Tool maintained by NYSDOH.

PPS Lead Organization entity that has been approved by NYSDOH and CMS to serve as designated organization that has assumed all responsibilities associated with DSRIP program per their project application and DSRIP award.

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 governed by a QE.

Qualified Health IT Entity ("QE") means a not-for-profit entity that has been certified as a QE under 10 N.Y.C.R.R. Section 300.4 and has executed a contract 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, queryable 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.

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

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

SHIN-NY Portal means the secure online website that gives patients and their Personal Representatives access to the Protected Health Information about them that is available through the SHIN-NY.

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)).

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 Participant shall not access a patient's Protected Health Information via the SHIN-NY governed by a QE unless the patient has provided an Affirmative Consent authorizing the Participant to access such Protected Health Information. An Affirmative Consent may be executed by an electronic signature as permitted by Section 1.8.5.
- 1.2 Exceptions to Affirmative Consent Requirement. Affirmative Consent shall not be required under the circumstances set forth in this Section 1.2.
 - 1.2.1 One-to-One Exchanges. Affirmative Consent shall not be required for a Participant to access a patient's Protected Health Information via the SHIN-NY governed by a QE from another Participant in a One-to-One Exchange provided the Participants comply with existing federal and state laws and regulations requiring patient consent for the disclosure

and re-disclosure of information by health care providers.¹

A health plan accessing clinical information for Quality Improvement or Care Management/coordination activities may constitute a one-to-one exchange between the participant and the health plan based on agreements in place between the provider and health plan. However, this exchange must comply with Section 1.8.13 which allows an individual to request to restrict 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), 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 Public Health Agency may access Protected Health Information through a QE's clinical viewer or portal 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);

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.

- 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) and the Health Emergency Response Data System (HERDS);
 - 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. A patient's denial of consent for all Participants in a QE to access the patient's Protected Health Information under Section 1.8.6 shall not prevent or otherwise restrict a Public Health Agency from accessing the patient's Protected Health Information through a QE for the purposes set forth in Section 1.2.2(b)(i)-(xvii).

1.2.3 Access for Disaster Tracking

- a. For the purpose of locating patients during an Emergency Event, a Disaster Relief Agency shall be allowed to access the following information through a QE 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. Access to information under this section may begin when the Emergency Event begins and shall cease when the Emergency Event ceases.
- c. Information accessed under this section shall not reveal the nature of the medical care received by the patient who is the subject of the access request 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 the patient's Protected Health Information under Section 1.8.6 shall not restrict a Disaster Relief Agency from accessing information as permitted by this section.

1.2.4 Emergency Access to PHI When Treating a Patient with an Emergency Condition or "Breaking the Glass."

- a. Affirmative Consent shall not be required for (i) a Practitioner; (ii) an Authorized User acting under the direction of a Practitioner; or (iii) an Advanced Emergency Medical Technician to access Protected Health Information via the SHIN-NY governed by a QE and these individuals may Break the Glass if the following conditions are met:
 - i. Treatment may be provided to the patient without informed consent because, in the Practitioner's or Advanced Emergency Medical Technician's judgment, an emergency condition exists and the patient is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the patient's life or health.
 - ii. The Practitioner or Advanced Emergency Medical Technician determines, in his or her reasonable judgment, that information that may be held by or accessible via the SHIN-NY governed by a QE may be material to emergency treatment.
 - iii. No denial of consent to access the patient's information is currently in effect with respect to the Participant with which the Practitioner, Authorized User acting under the direction of a Practitioner or Advanced Emergency Medical Technician is affiliated.
 - iv. In the event that an Authorized User acting under the direction of a Practitioner -Breaks the Glass, such Authorized User must record the name of the Practitioner providing such direction.
 - v. The Practitioner, Advanced Emergency Medical Technician or Authorized User acting under the direction of a Practitioner attests that all of the foregoing conditions have been satisfied, and the QE software maintains a record of this access.
- b. Emergency PHI access by an Authorized User acting under the direction of a

Practitioner must be granted by a Practitioner on a case by case basis.

- c. QEs shall ensure, or shall require their Participants to ensure, that access to information via the SHIN-NY governed by a QE without Affirmative Consent when treating a patient pursuant to this Section 1.2.4 terminates upon the completion of the emergency treatment.
- d. Notwithstanding anything to the contrary set forth in these policies, a QE and its Participants shall not be required to exclude any Sensitive Health Information from access via the SHIN-NY governed by a QE where the circumstances set forth in this Section 1.2.4 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 accessed through the QE under this Section 1.2.4. This notice shall include (i) the name of the Participant that accessed the Protected Health Information; (ii) the name of the Authorized User within the Participant that accessed the Protected Health Information; (iii) the date and time of the access; and (iv) the nature of the emergency.
- f. Upon a patient's discharge from a Participant's emergency room, if emergency access to PHI occurred during the emergency room visit, the Participant shall notify the patient of such incident and inform the patient how he or she may request an audit log in accordance with Section 6.4 of these P&Ps. In lieu of providing such notice, Participants that are hospitals may notify all patients discharged from an emergency room that their PHI may have been accessed during a Break the Glass incident and inform patients how they may request an audit log to determine if such access occurred. The notice required by this Section shall be provided within ten days of the patient's discharge and may be provided by the QE on behalf of the Participant.

1.2.5 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 make the information accessible to Participants 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 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 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 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 Protected Health Information via the SHIN-NY governed by a QE for the purpose of evaluating and improving QE operations.
- 1.2.7 The provisions of this Section 1.2.6 do not permit QEs to access Protected Health Information without a Level 2 Consent for Research. However, QEs may access De-Identified Data without Affirmative Consent for the purposes set forth in Section 1.6 or a Limited Data Set for the purposes set forth in Section 1.7. Consistent with HIPAA, access to PHI should be limited to the minimum amount necessary to accomplish the intended purpose of the use or disclosure.
- 1.2.8 De-Identified Data. Affirmative Consent shall not be required for access to De-identified Data for specified uses as set forth in Section 1.6.
- 1.2.9 Organ Procurement Organization Access. A QE may provide an Organ Procurement Organization with access to Protected Health Information without Affirmative Consent solely for the purposes of facilitating organ, eye or tissue donation and transplantation. A patient's denial of Affirmative Consent for all Participants in a QE to access the patient's Protected Health Information under Section 1.8.6 shall not prevent or otherwise restrict an Organ Procurement Organization from accessing the patient's Protected Health Information through a QE for the purposes set forth in this Section 1.2.8.
- 1.3 Form of Patient Consent. Except as otherwise permitted by the Patient Consent Transition Rules set forth at Section 1.9, consents shall be obtained through an Approved Consent. A QE may request approval to use a consent other than a Level 1 Consent or Level 2 Consent if it obtains approval from NYSDOH. Such approval will not be granted unless the alternative consent is substantially similar to the Level 1 Consent or Level 2 Consent, as applicable, and achieves the same basic purposes as such consents, as set forth in these Policies and Procedures.
 - 1.3.1 Level 1 Uses. Affirmative Consent to access information via the SHIN-NY governed by a QE for Level 1 Uses shall be obtained using a Level 1 Consent or an alternative approved by NYSDOH under Section 1.3, which shall include the following information:
 - a. The information to which the patient is granting the Participant access, including specific reference to HIV, mental health, alcohol and substance abuse, reproductive health, sexually-transmitted disease, and genetic testing information;
 - b. The intended uses to which the information will be put by the Participant;
 - c. The relationship between the Participant and the patient whose information will be accessed;
 - d. A list of or reference to all Data Suppliers at the time of the patient's consent, as well as an acknowledgement that Data Suppliers may change over time and instructions for patients to access an up-to-date list of Data Suppliers through a QE website or other means; the consent form shall also identify whether the QE is party to data sharing agreements with other QEs and, if so, provide instructions for patients to access an up-to-date list of Data Suppliers from a QE website or by other means;

- e. Certification that only those engaged in Level 1 Uses may access the patient's information;
- f. Acknowledgement of the patient's right to revoke consent and assurance that treatment will not be affected as a result;
- g. Whether and to what extent information is subject to re-disclosure;
- h. The time period during which the consent is to be effective;
- i. The signature of the patient or the patient's Personal Representative;
- and,
- j. The date of execution of the consent.

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

- a. The specific purpose for which information is being accessed;
- b. Whether the QE and/or its Participants will benefit financially as a result of the use/disclosure of the information to which the patient granting access;
- c. The date or event upon which the patient's consent expires;
- d. Acknowledgement that payers may not condition health plan enrollment and receipt of benefits on a patient's decision to grant or withhold consent.

1.3.3 Requirement for Separate Consents

- a. Consent for Level 1 Uses and consent for Level 2 Uses shall not be combined.
- b. Consent for different Level 2 Uses shall not be combined.
- c. A Consent for a Level 1 or Level 2 Use shall not be combined with any other document except with the approval of NYSDOH.

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

1.4 Sensitive Health Information

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

1.4.2 Withholding Sensitive Health Information. QEs and Participants may, but shall not be

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

1.4.3 Re-disclosure Warning

- a. QEs shall include a warning statement that is viewed by Authorized Users whenever they are obtaining access to records of federally-assisted alcohol or drug abuse programs regulated under 42 C.F.R. Part 2 that contains the language required by 42 C.F.R. § 2.32. A QE may satisfy this requirement by placing such a 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 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 re-disclosure warning on a log-in screen that Authorized Users must view before logging into their EHR or otherwise accessing the QE.
- c. QEs shall include a warning statement that is viewed by Authorized Users whenever they are obtaining access to records of facilities licensed or operated by the New York State Office of Mental Health or the New York State Office for People With Developmental Disabilities that contains language notifying the Authorized User that such records may not be re-disclosed 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 re-disclosure warning required at Section 1.4.3(a) or (ii) placing such a re-disclosure 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 abuse information, and records of facilities licensed or operated by the New York State Office of Mental Health or the New York State Office for People With Developmental Disabilities.

1.5 Special Provisions Relating to Minors.

1.5.1 A Participant may access through the SHIN-NY Protected Health Information about minors – other than Minor Consent Information – based on an Affirmative Consent executed by the minor's Personal Representative.

1.5.2 A Participant may access Minor Consent Information through the SHIN-NY 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 such information without the minor's Affirmative Consent.

1.5.3 Notwithstanding Section 1.5.2, QEs and their Participants may not disclose Minor Consent Information to the minor's Personal Representative without the minor's written consent. QEs must provide or arrange for training for their Participants on compliance with this Section 1.5.3.

1.6 De-Identified Data.

1.6.1 Access of De-Identified Data for Specified Uses.

- a. Affirmative Consent shall not be required for a QE, a Participant, or a government agency to access De-Identified Data via the SHIN-NY governed by a QE for Research in accordance with Section 1.7.1.
- b. Affirmative Consent shall not be required for a Participant to access De-Identified Data via the SHIN-NY for Quality Improvement, provided that a specially designated committee appointed by the QE reviews and approves the Quality Improvement activity in accordance with standards. Participants must make available to the committee the methodology of any proposed Quality Improvement project, which the QE shall make accessible to other Participants and the general public.
- c. Affirmative Consent shall not be required for a QE, a Participant, or a government agency to access De-Identified Data via the SHIN-NY for any purpose for which the QE, Participant, or government agency may lawfully access Protected Health Information under the Policies and Procedures;
- d. Affirmative Consent shall not be required for a QE to perform an evaluation of the economic or other value of the QE provided that the methodology and results of any such evaluation are posted on the QE's website.

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

1.6.3 Other Requirements-

- a. All other uses of De-Identified Data shall require Affirmative Consent.
- b. A QE shall not condition a patient's participation in the QE on the patient's decision to consent or deny access to De-Identified Data for purposes other than those set forth in Section 1.6.1.
- c. QEs shall, or shall require Participants to, comply with standards for the de-identification of data set forth in 45 C.F.R. § 164.514.
- d. QEs shall, or shall require Participants or government agencies to, subject any

use of De-Identified Data to adequate restrictions on the re-identification of such data.

1.7 Research

- 1.7.1 Use of De-Identified Data for Research. Affirmative Consent shall not be required for a QE or a Participant to access De-Identified Data via the SHIN-NY in order to conduct Research approved or deemed exempt by an Institutional Review Board organized and operating in accordance with 45 C.F.R. § 164.
- 1.7.2 Use of Limited Data Set for Research. Affirmative Consent shall not be required for a QE or a Participant to access a Limited Data Set in order to conduct Research approved or deemed exempt by an Institutional Review Board organized and operating in accordance with 45 C.F.R. § 164.
- 1.7.3 Review of Exempt Research by QE Committee. If proposed Research using De-Identified Data or a Limited Data Set is deemed exempt by an Institutional Review Board under Section 1.7.1 or 1.7.2, the Participant seeking to perform the Research shall obtain approval for the Research from the committee appointed by the QE under Section 1.6.1(b). The committee shall apply standards for such reviews adopted through the SCP. Participants must make available to the committee the methodology of any proposed Research project, which the QE shall make accessible to other Participants and the general public.
- 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 or 1.7.2.

1.8 Other Policies and Procedures Related to Consent.

- 1.8.1 Affiliated Practitioners. An Affirmative Consent obtained by a Participant shall apply to an Affiliated Practitioner of the Participant provided that (i) such Affiliated Practitioner is providing health care services to the patient at the Participant's facilities; (ii) such Affiliated Practitioner is providing health care services to the patient in his or her capacity as an employee or contractor of the Participant or (iii) such Affiliated Practitioner is providing health care services to the patient in the course of a cross-coverage or on-call arrangement with the Participant or one of its Affiliated Practitioners.
- 1.8.2 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.
- 1.8.3 QEs and Participants may use Affirmative Consents that apply to more than one Participant, subject to the following conditions.
 - a. The Participant 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 that Participant.
 - b. If the multi-Participant consent allows a Participant to access 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 notifies patients that the list of Participants will be regularly updated on the QE's website and that patients have a right to obtain a hard copy of the list, free of charge, upon request, 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.

- 1.8.4 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.
- 1.8.5 Electronic Signatures. Affirmative Consent may be obtained electronically provided that there is an electronic signature that meets the requirements of the federal E-SIGN 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 NYCRR Part 540, New York State Office of Information Technology Services ESRA Guidelines NYS-G04-001).
- 1.8.6 Denial of Consent. Consents shall give the patient the option of granting or affirmatively denying consent for individual Participants to access information about the patient via the SHIN-NY governed by a QE. A patient's decision not to sign a consent shall not be construed as a "denial of consent" under Section 1.2.4(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 QE to access the patient's information, except as set forth in Section 1.2.2(b) or Section 1.2.8.
- 1.8.7 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.
- 1.8.8 Revocability. Patients shall be entitled to revoke an Affirmative Consent at any time provided that such revocation shall not preclude any Participant that has accessed Protected Health Information via the SHIN-NY governed by a QE prior to such revocation and incorporated such Protected Health Information into its records from retaining such information in its records.
- 1.8.9 Notification of a QE's Data Suppliers. QEs shall provide, or shall require their Participants to provide, patients with a list of or reference to all Data Suppliers at the time the QE or Participant obtains the patient's Affirmative Consent. Each QE shall provide convenient access at all times thereafter, either through its website or otherwise, to a complete and accurate updated list of Data Suppliers.

- 1.8.10 Compliance with Business Associate Agreements with Data Suppliers. A QE shall execute a Business Associate Agreement with each Data Supplier. A QE shall not use or disclose Protected Health Information in any manner that violates the QE's Business Associate Agreements.
- 1.8.11 Disclosure to Vendors. A QE, acting under the authority of a Business Associate Agreement with its Participants, may disclose Protected Health Information to vendors that assist in carrying out the QE's authorized activities provided (i) the QE requires the vendors to protect the confidentiality of the Protected Health Information in accordance with the QE's Business Associate Agreements with its Participants and (ii) the vendor does not make such information available to a Participant that has not obtained Affirmative Consent.
- 1.8.12 Compliance with Existing Law. All access to Protected Health Information via the SHIN-NY governed by a QE shall be consistent with applicable federal, state and local laws and regulations. If applicable law requires that certain documentation exist or that other conditions be met prior to accessing Protected Health Information for a particular purpose, Participants shall ensure that they have obtained the required documentation or met the requisite conditions and shall provide evidence of such as applicable.
- 1.8.13 Compliance with Requests for Restrictions on Disclosures to a Payer Organization. QEs shall develop processes to ensure that a Payer Organization does not access Protected Health Information through the QE if a patient has requested, in accordance with the HIPAA Privacy Rule and HITECH, that the Provider Organization creating such information not disclose it to the Payer Organization. While a QE may utilize any process that satisfies this requirement, a QE shall be deemed to have complied with the requirement if:
- a. Upon a Provider Organization's receipt of a patient's request that Protected Health Information created by the Provider Organization not be disclosed to a Payer Organization, any Affirmative Consent previously granted to such Payer Organization is revoked and such revocation remains in effect permanently unless and until the patient's request is withdrawn; and
 - b. Upon receipt of an Affirmative Consent covering a Payer Organization, the Payer Organization or QE notifies the patient in writing that his or her provision of the Affirmative Consent will revoke any prior request for a restriction on the disclosure of Protected Health Information by any Provider Organization to the Payer Organization, and the Affirmative Consent is rejected if the patient indicates he or she does not agree to the revocation of his or her prior request.
- 1.8.14 Development of Policies Governing Disclosures to Government Agencies for Health Oversight. QEs shall adopt policies governing the QE's response to requests from government agencies for access to Protected Health Information for health oversight purposes, such as Medicaid audits, professional licensing reviews, and fraud and abuse investigations. Such policies shall address whether the QE will disclose information without Affirmative Consent in instances where disclosure is permitted but not required by law, and whether the QE will notify its Participants of such requests. This section does not cover access to Protected Health Information by Public Health Agencies under Section 1.2.2.
- 1.8.15 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.

- 1.8.16 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.

1.9 Patient Consent Transition Rules.

- 1.9.1 Use of Approved Consents. Except as set forth in Section 1.9.2, each QE shall be required to utilize an Approved Consent with respect to all patients who consent to the exchange of Protected Health Information via the SHIN-NY governed by a QE on or after the Consent Implementation Date.

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

- 1.9.3 Use of Existing Consent After Consent Implementation Date. A QE may continue to use an Existing Consent after the Consent Implementation Date if the Existing Consent is approved by NYSDOH under Section 1.3.

1.10 Receipt of Patient Care Alerts.

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

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

SECTION 2: AUTHORIZATION

Purpose/Principles

Authorization is the process of determining whether a particular individual within a Participant has the right to access Protected Health Information via the SHIN-NY governed by a QE. Authorization is based on role-based access standards that take into account an individual’s job function and the information needed to successfully carry out a role within the Participant. Section 2 sets forth minimum requirements that QEs and their Participants shall follow when establishing role-based access standards and authorizing individuals to access information about a patient via the SHIN-NY governed by a QE. They are designed to limit exchange of information to the minimum 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 governed by a QE; and
- c. Define the types of Protected Health Information that Authorized Users within such categories may access (e.g., demographic data only, clinical data).

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

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

- a. Emergency access or "Break the Glass" - a (i) Practitioner; (ii) Authorized User acting under the direction of a Practitioner; or (iii) Advanced Emergency Medical Technician who, under the provisions of §1.2.3 ('Break the Glass') has temporary rights to access Protected Health Information for a specific patient;
- b. Practitioner with access to clinical and non-clinical information;
- c. Non-Practitioner with access to clinical and non-clinical information;
- d. Non-Practitioner with access to non-clinical information;
- e. QE administrators with access to non-clinical information;
- f. QE administrators with access to clinical information in order to engage in public health reporting in accordance with Section 1.2.2 of these Policies and Procedures or other activities authorized under these Policies and Procedures; and
- g. QE or Participant administrators with access to clinical and non-clinical information for purposes of system maintenance and testing, troubleshooting and similar operational and technical support purposes.

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

2.1.5 QEs and Participants shall identify individuals (including individuals encompassed within the role-based access category defined at §2.1.3(g)) whose access to data may bypass or enable circumvention of activity logging, access controls, or other security controls. These

Authorized Users shall be subject to heightened scrutiny both in hiring and in ongoing auditing and monitoring of their activities. Such heightened scrutiny may include -pre-employment (or pre-engagement for contractors) background checks; mandatory privacy and security training and annual retraining; a formal termination procedure more stringent and timely than that set forth in §4.8; regular review of access privileges, user accounts; or other measures as the QE or Participant may deem appropriate given their security risk assessment.

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

SECTION 3: AUTHENTICATION

Purpose/Principles

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

Policies and Procedures

- 3.1 **Obligation to Ensure Authentication of Identity of Authorized User Prior to Access.** QEs shall authenticate, or shall require their Participants to authenticate, each Authorized User's identity prior to providing such Authorized User with access to Protected Health Information via the-SHIN-NY governed by a QE. Such authentication shall take place in accordance with the provisions of this Section 3.
- 3.2 **Authentication Requirements.**
 - 3.2.1 **Authentication Standard.** Until such time as a determination is made, pursuant to Section 3.2.2, to utilize a higher authentication standard, QEs shall authenticate, or shall require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Identity Level of Assurance 2 ("Level 2") set forth in National Institute of Standards and Technology Special Publication 800-63 (hereinafter, "NIST SP 800-63").
 - a. Level 2 will require, among other technical specifications, QEs or their Participants to authenticate each Authorized User's identity using only single-factor authentication, which queries Authorized Users for something they know (e.g., a password). Under Level 2, QEs or their Participants will be free to use only a password, and need not use it in combination with any other tokens, provided it protects against online guessing and replay attacks. Level 2 will require QEs or their Participants to implement initial identity-proofing procedures (either remote or in- person) that require Authorized Users to provide identifying materials and information upon application for access to information through the

QE.

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

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

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

- 3.3 Compliance with Policies Resulting from Statewide Risk Analysis. In the event that New York State conducts a statewide risk analysis of the potential harm and likelihood of adverse impacts that could result from an error in identity authentication within the SHIN-NY that indicates that authentication policies and procedures that differ from, or are in addition to, those set forth in this Section 3, should be adopted, any such authentication policies and procedures shall be developed and approved through the SCP before adoption.
- 3.4 Option to Rely on Statewide Authentication Service. In the event that New York State develops statewide services for the authentication of Authorized Users, QEs may utilize such statewide services to authenticate an Authorized User in accordance with the provisions of this Section 3.
- 3.5 Authentication of Certified Applications and Downstream Users. QEs permitting access to the SHIN-NY by Participants through Certified Applications must (i) implement systems consistent with the SHIN-NY Policy Standards for authenticating a Certified Application's credentials in connection with each access request; and (ii) require each Participant accessing Protected Health Information through a Certified Application to authenticate the Participant's users in a manner consistent with Section 3 of these Policies and Procedures.

SECTION 4: ACCESS

Purpose/Principles

Access controls govern when and how a patient's information may be accessed by Authorized Users through a QE's Participant. This Section 4 sets forth minimum behavioral controls QEs shall implement to ensure that:

1.) Only Authorized Users and Certified Applications access information via the SHIN-NY governed by a QE; and 2.) they do so only in accordance with patient consent and with other requirements (specified herein) that limit their access to specified information (e.g., that which is relevant to a patient's treatment). These access policies, coupled with informed patient consent, are designed to reduce unauthorized access and ensure information is used for authorized purposes.

Policies and Procedures

- 4.1 General. QEs shall, or shall require their Participants to, ensure that each Authorized User is (i) assigned a unique user name and password to provide such Authorized User with access to patient information via the SHIN-NY governed by a QE 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 NIST SP 800-63 (e.g. the probability of success of an online password guessing attack shall not exceed 1 in 16,384 over the life of the password).
 - 4.1.3 Group or temporary user names shall be prohibited.
 - 4.1.4 Authorized Users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing passwords.
 - 4.1.5 Authorized Users shall be prohibited from sharing their user names, passwords or other authentication tools (e.g., tokens), with others and from using the user names, 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 governed by a QE only for purposes consistent with a patient's Affirmative Consent or an exception set forth in Section 1.2
- 4.3 Failed Access Attempts. QEs shall enforce a limit of consecutive Failed Access Attempts by an Authorized User. Upon a fifth Failed Access Attempt, QEs shall ensure that said Authorized User's access to the QE is disabled either by locking the account until release by a QE administrator or by locking the account for a specific period of time as specified by the QE, after which the Authorized User may reestablish access using appropriate identification and authentication procedures. If Authorized Users access the SHIN-NY governed by a QE by logging on to a Participant's information system (without the need for a separate QE log-on), the QE may delegate to the Participant responsibility for enforcing this Failed Access Attempt limitation.
- 4.4 Periods of Inactivity. QEs shall ensure that an Authorized User is automatically logged out of the QE after a period of inactivity by such Authorized User. The termination shall remain in effect until the Authorized User reestablishes access using appropriate identification and authentication procedures. QEs shall establish the length of periods of inactivity that will trigger such termination based on their internal risk analyses as well organizational factors such as current technical infrastructure, hardware and software security capabilities.

- 4.5 Access Limited to Minimum Necessary Information. QEs shall, and shall require their Participants to, ensure that reasonable efforts are made, except in the case of access for Treatment, to limit the information accessed via the SHIN-NY governed by a QE to the minimum amount necessary to accomplish the intended purpose for which the information is accessed.
- 4.6 Record Locator Service and Other Comparable Directories. In operating a Record Locator Service or Other Comparable Directory, QEs shall, or shall require their Participants to:
- 4.6.1 Implement reasonable safeguards to minimize unauthorized incidental disclosures of Protected Health Information during the process of identifying a patient and locating a patient's medical records.
- 4.6.2 Include the minimum amount of demographic information reasonably necessary to enable Authorized Users to successfully identify a patient through the Record Locator System.
- 4.6.3 Prohibit Authorized Users from accessing Protected Health Information in any manner inconsistent with these Policies and Procedures.
- 4.7 Training. The behavioral and organizational access controls set forth above will only be effective if:
- 1.) A QE's health information access policies and procedures are clear; and 2.) Authorized Users understand the policies and procedures and their responsibilities within such policies and procedures. As such, QEs shall implement, either directly or through Participants, minimum training requirements for educating individuals about the policies and procedures for accessing Protected Health Information via the SHIN-NY governed by a QE as specified by the Statewide Collaboration Process. 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 governed by a QE.
- 4.7.2 QEs shall, or shall require their Participants to, ensure that each Authorized User undergoes such training prior to being granted access to information via the SHIN-NY governed by a QE.
- 4.7.3 QEs shall, or shall require their Participants to, ensure that each Authorized User signs a certification that he or she has received training and will comply with the QE's policies and procedures. Such certification may be made on a paper form or electronically and shall be retained by QEs or their Participants for at least six years.
- 4.7.4 QEs shall, or shall require their Participants to, ensure that each Authorized User undergoes continuing and/or refresher training on an annual basis as a condition of maintaining authorization to access patient information via the SHIN-NY governed by a QE. QEs shall ensure that records of such training are maintained and available for audit for a period of at least six years.
- 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.

4.8.1 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.

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

4.9 Access by Certified Applications.

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

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

4.9.3 The QE shall require a Participant using a Certified Application to limit access to any Protected Health Information obtained through the Certified Application to individual users of the Participant's information system who would be eligible to be Authorized Users of the Participant under these Policies and Procedures if they were accessing Protected Health Information directly through the QE. The QE shall also require the Participant to credential, train and otherwise manage the access of such users to Protected Health Information obtained through the QE in accordance with the provisions of this Section 4 applicable to Authorized Users.

4.10 Participation Agreements

- 4.10.1 Except as set forth otherwise in Section 4.10.2, a QE shall enter into a Participation Agreement directly with each of its Participants. Participation Agreements shall require Participants to comply with these Policies and Procedures, as they may be amended from time to time.
- 4.10.2 A QE may enter into a Participation Agreement with a Provider Organization that covers Practitioners participating in an electronic health information exchange maintained by the Provider Organization if:
- a. The Provider Organization enters into a written agreement with each Practitioner or medical group comprised of Practitioners in a form acceptable to the QE that obligates the Practitioner(s) to abide by the relevant terms of the Provider Organization's Participation Agreement with the QE and engage in bi-directional exchange of Protected Health Information through the SHIN-NY.
 - b. The Provider Organization, under its Participation Agreement with the QE, assumes responsibility for the training and oversight of the Practitioners under these Policies and Procedures as if the Practitioners were Authorized Users of the Provider Organization.
 - c. The Provider Organization, under its Participation Agreement with the QE, accepts liability for the acts and omissions of such Practitioners for violations of the Provider Organization's Participation Agreement with the QE as if such Practitioners were Authorized Users of the Provider Organization.
- 4.10.3 Notwithstanding a Provider Organization's responsibilities with respect to Practitioners participating in a QE through the Provider Organization under Section 4.10.2, each Practitioner or medical group entering into a written agreement with the Provider Organization shall be treated as a separate Participant for purposes of implementing the patient consent requirements of these Policies and Procedures.
- 4.10.4 Sections 4.10.2 and 4.10.3 shall not apply to Practitioners when they are acting as Affiliated Practitioners of a Provider Organization under Section 1.8.1.

SECTION 5: PATIENT 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 his or her Protected Health Information. QEs present an opportunity for patients to gain access to their health information in an electronic format through a single electronic portal. Such access would eliminate or 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 governed by a QE is a foundational principle essential to protecting patient privacy and to realizing the potential for QEs to markedly improve patient access to their own health information. This Section 5 sets forth minimum 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 QEs shall be required to educate patients and/or their Personal Representatives with respect to the consent process and the terms and conditions upon which their Protected Health Information can be shared with Authorized Users, including conforming to any patient education program standards developed through the SCP, and informing the patient and/or his or her Personal Representative of the benefits and risks of providing an Affirmative Consent for his or her Protected Health Information to be shared through the QE.
- 5.2 QEs shall facilitate the access of patients and their Personal Representatives to the patient's Protected Health Information through (i) the mechanism set forth in Section 5.2.3 and (ii) either the mechanism set forth in Section 5.2.1 or the mechanism set forth in Section 5.2.2. Each patient shall have the right to indicate which of the mechanisms offered by the QE he or she prefers to utilize to obtain access to his or her information. . Notwithstanding the foregoing, a QE shall not be required to provide access to Protected Health Information through any individual mechanism until all of the implementation contingencies associated with that mechanism have been satisfied. The date by which QEs must make the mechanism available shall be established through the SCP but may not be more than 180 days after the date on which all of the implementation contingencies associated with that mechanism have been satisfied. The implementation contingencies for each mechanism are the adoption of standards through the SCP applicable to that mechanism governing (i) the nature and scope of the Protected Health Information that must be made accessible to patients and their Personal Representatives, (ii) the timing of the provision of such access; and (iii) identity proofing and authentication of patients and their Personal Representatives, QEs shall comply with all such standards when they become effective. Nothing in this Section 5.2 shall prohibit a QE from voluntarily providing patients or their Personal Representatives with access to Protected Health Information through any means compliant with applicable law prior to the effective date of the requirements set forth herein. The QE shall inform patients or their Personal Representatives, as appropriate, about the means through which they may access their Protected Health Information and all material terms and conditions regarding such access.
- 5.2.1 A QE may facilitate access to Protected Health Information through the SHIN-NY Portal if operational.
- 5.2.2 A QE may facilitate access to Protected Health Information through its own web-based portal or through Participants' patient web-based portals, provided that each such portal enables access to information maintained by the QE on behalf of all of its Participants.
- 5.2.3 A QE shall facilitate access to Protected Health Information by providing a paper or electronic copy of information maintained about the patient by the QE. Each patient shall have the right to indicate whether he or she prefers to receive information in paper or electronic form.
- 5.3 A QE and its Participants may (but are not required to) allow patients to grant access to their Protected Health Information to family members, informal caregivers and friends of the patient who are not Personal Representatives, provided such access is in accordance with any privacy and security standards.
- 5.4 Access of patients, their Personal Representatives, their family members, their informal caregivers and their friends who are not Personal Representatives to Protected Health Information must be in accordance with all applicable laws and regulations, including but not limited to, PHL §18, MHL § 33.16 and 10 NYCCR § 58-1.8. As well as laws granting minors the right to keep Minor Consent Information confidential from their parents or guardians.

Notwithstanding Section 5.2, if a QE does not have a practical means of ensuring that Minor Consent Information can be segregated or otherwise filtered from other Protected Health Information about minors, the QE may deny Personal Representatives of minors between the ages of 10 and 17 with access to all of the minor's Protected Health Information.

- 5.5 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 (i) notice -in a manner easily understood by patients – that their Protected Health Information is being uploaded to a QE; (ii) a list of or reference to all Data Suppliers (consistent with Section 1.8.9); (iii) information about how to contact Data Suppliers; and (iv) a description of how patients may deny consent for all QE Participants to access their Protected Health Information through the QE in accordance with Section 1.8.6. QEs and their Participants shall participate in any applicable patient education programs developed through the SCP for the purpose of educating patients about the uploading of their Protected Health Information to a QE.
- 5.6 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.
- 5.7 As required in Section 6.4, QEs shall, or shall require their Participants to, provide patients with information about how their Protected Health Information was accessed through the QE.
- 5.8 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.
- 5.9 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.
- 5.10 Each QE shall make reasonable efforts to provide its Participants with information indicating which other QE Participants have accessed erroneous information that the Participant has corrected at the request of patients in accordance with Section 5.8.

SECTION 6: AUDIT

Purpose/Principles

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

Policies and Procedures

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

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

- a. The identity of the patient whose Protected Health Information was accessed;
- b. The identity of the Authorized User accessing the Protected Health Information;
- c. The identity of the Participant with which such Authorized User is affiliated;
- d. The type of Protected Health Information or record accessed (e.g., pharmacy data, laboratory data, etc.);
- e. The date and time of access;
- f. The source of the Protected Health Information (i.e., the identity of the Participant from whose records the accessed Protected Health Information was derived); and
- g. Unsuccessful access (log-in) attempts; and
- h. Whether access occurred through a Break the Glass incident.

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

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

6.1.4 Audit Logs shall be immutable. An immutable Audit Log requires either that log information cannot be altered by anyone regardless of access privilege or that any alterations are tamper evident.

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

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

6.2.1 At a minimum, the QE shall audit, or require its Participants to audit, the following:

- a. That Affirmative Consents are on file for patients whose Protected Health Information is accessed via the SHIN-NY governed by a QE, other than in Break the Glass situations;
- b. That Authorized Users who access Protected Health Information via the SHIN-

NY governed by a QE do so for Authorized Purposes; and

c. That applicable requirements were met where Protected Health Information was accessed through a Break the Glass incident.

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

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

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

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

6.2.6 If audits are conducted by Participants rather than by the QE, the QE shall:

a. Require each Participant to conduct the audit within such time period as reasonably requested by the QE; and

b. Require each Participant to report the results of the audit to the QE within such time period and in such format as reasonably requested by the QE.

6.3 Participant Access to Audit Logs.

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

a. The name of each Authorized User who accessed such patient's Protected Health Information in the prior 6-year period;

b. The time and date of such access; and

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

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

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

6.4 Patient Access to Audit Information.

6.4.1 Each QE shall provide patients, upon request, with the following information:

- a. The name of each Participant that accessed the patient's Protected Health Information in up to the prior 6-year period;
 - b. The time and date of such access; and
 - c. The type of Protected Health Information or record that was accessed (e.g., clinical data, laboratory data, etc.).
- 6.4.2 If a patient requests the name(s) of the Authorized User(s) who accessed his or her 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; 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 governed by a QE.
- 6.4.4 If applicable, QEs shall, or shall require their Participants to, provide notice of the availability of such information on any patient portals maintained by the QE or its Participants.
- 6.5 **Public Availability of Audits.** Each QE shall make the results of its periodic audit available on the QE's website. Such results shall be made available as promptly as reasonably practicable, but in any event not more than 30 days after completion of the audit.
- 6.6 **Correction of Erroneous Data.** In the most expedient time possible each QE shall investigate (or require the applicable Participant to investigate) the scope and magnitude of any data inconsistency or potential error that was made in the course of the QE's data aggregation and

exchange activities and, if an error is determined to exist, identify the root cause of the error and ensure its correction. QEs shall log all such errors, the actions taken to address them and the final resolution of the error. QEs shall also make reasonable efforts to identify Participants that accessed such erroneous information and to notify them of corrections. This provision does not apply to updates to data that are made by Data Suppliers in the ordinary course of their clinical activities nor does it apply to updates to Demographic Information.

- 6.7 Weekly Audit Reports by Organ Procurement Organizations. QEs shall require weekly confirmation by Organ Procurement Organizations that all instances in which Protected Health Information was accessed through the QE by the Organ Procurement Organization's Authorized Users were consistent with the terms of these Policies and Procedures (based upon a listing sent by the QE).
- 6.8 Additional Requirements Related to Auditing of Public Health Access. QEs shall use special safeguards with respect to audits of access by Public Health Agencies, which shall include at least the following:
 - 6.8.1 The QE shall create, on a regular basis, an audit report of Authorized User activity for each Public Health Agency workgroup that will include, at a minimum, the patient names, times, dates and reason for access for each Authorized User.
 - 6.8.2 The name of the particular Public Health Agency shall be listed in the patient audit logs.
 - 6.8.3 The QE shall follow-up with workgroup manager(s) if approval of an audit report is not received. If the attempt to contact the workgroup manager(s) is unsuccessful, the QE may suspend all Authorized User accounts associated with that particular workgroup until the situation is resolved.

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 via the SHIN-NY governed by a QE.
 - 7.1.1 Notification shall be made in the most expedient time possible and without unreasonable delay.
 - 7.1.2 Notification shall be made in writing.
- 7.2 Responsibilities of the QE.

- 7.2.1 QEs shall be required to develop a Breach plan as part of their policies and procedures. The plan shall provide that, in the event the QE becomes aware of any suspected Breach of Unsecured Protected Health Information, either through notification by a Participant or otherwise, the QE must, in the most expedient time possible and without unreasonable delay, investigate (or require the applicable Participant to investigate) the scope and magnitude of such suspected Breach, determine whether an actual Breach has occurred and, if so, identify the root cause of the Breach.
- 7.2.2 In the event it is determined that an actual Breach has occurred, the QE must, at a minimum:
- a. Notify any Participants whose Protected Health Information was subject to the Breach.
 - b. Mitigate (or require the applicable Participant to mitigate) to the extent practicable, any harmful effect of such Breach that is known to the QE or the Participant. QEs' mitigation efforts shall correspond with and be dependent upon their internal risk analyses. Notify (or require the applicable Participant to notify) the patient and any applicable regulatory agencies as required by and in accordance with applicable federal, state and local laws and regulations, including but not limited to HITECH.

SECTION 8: HIPAA COMPLIANCE

Purpose/Principles

While it is anticipated that most Participants will be Covered Entities and thus subject to the HIPAA Privacy Rule and HIPAA Security Rule, there may be some Participants that are not Covered Entities. The provisions of this Section 8 are designed to ensure that entities that are not Covered Entities, other than a public health authority or a health oversight agency under HIPAA (45 CFR Sections 164.501 and 164.512(b) and (d)), accessing Protected Health Information through a QE abide by the same applicable HIPAA requirements as Covered Entities even if they are not otherwise legally obligated to do so.

Policies and Procedures

- 8.1 Each Participant that is a Covered Entity shall comply with the HIPAA Privacy Rule and HIPAA Security Rule.
- 8.2 Each Participant that is not a Covered Entity, other than a public health authority or a health oversight agency under HIPAA (45 CFR Sections 164.501 and 164.512(b) and (d)), shall adopt/address all of the applicable administrative, physical and technical safeguards set forth in the HIPAA Security Rule as well as the restrictions on the use and disclosure of Protected Health Information set forth in the HIPAA Privacy Rule.

SECTION 9: SANCTIONS

Purpose/Principles

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

these Policies & Procedures. The provisions in this Section 9 are designed to provide guidelines for the imposition of sanctions by QEs and their Participants while leaving flexibility for QEs and their Participants to determine appropriate sanctions on a case by case basis.

Policies and Procedures

- 9.1 Each QE shall establish policies consistent with this Section 9 governing the imposition of sanctions on Participants and their Authorized Users who violate the terms of these Policies and Procedures. QEs shall apply, or require their Participants to apply, sanctions under such policies in the event of such violations. QEs and/or their Participants and Public Health Agencies shall inform all Authorized Users about the QE's sanctions policies.
- 9.2 When determining the type of sanction to apply, QEs and/or their Participants shall take into account the following factors: (i) whether the violation was a first time or repeat offense; (ii) the level of culpability of the Participant or Authorized User, e.g., whether the violation was made intentionally, recklessly or negligently; (iii) whether the violation constitutes a crime under state or federal law; and (iv) whether the violation resulted in harm to a patient or other person.
- 9.3 Sanctions shall include, but do not necessarily have to be limited to: (i) requiring an Authorized User to undergo additional training with respect to participation in the QE; (ii) temporarily restricting an Authorized User's access to the QE; (iii) terminating the access of an Authorized User to the QE; (iv) suspending or terminating a Participant's participation in the QE; and (v) the assessment of fines or other monetary penalties.

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

Available on the NYSDOH Website.

Appendix A

Attachment A-1

Authorization for Access to Patient Information

New York State Department of Health

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.

<p>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.</p>
<p><input type="checkbox"/> 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.</p>
<p><input type="checkbox"/> 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.</p>

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].

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
- 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

Authorization for Access to Patient Information

New York State Department of Health

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.

<p>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.</p>
<p><input type="checkbox"/> 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).</p>
<p><input type="checkbox"/> 2. I DENY CONSENT EXCEPT IN A MEDICAL EMERGENCY for</p>

[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].

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

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.