Privacy and Security Policies and Procedures for RHIOs and their Participants in New York State

Version 1.1

Introduction

This document ("RHIO Privacy and Security Policies and Procedures – V1.1" or "Policies and Procedures") sets forth Version 1.1 of the Policies and Procedures governing interoperable health information exchange via the Statewide Health Information Network for New York ("SHIN-NY") facilitated by regional health information organizations ("RHIOs") in New York State. Version 1.1 reflects the following changes from Version 1.0:

- Updates to Section 1.5 "Special Provisions Relating to Minors," enabling RHIOs and their Participants to permit the exchange of information about minors below ten years of age based on an Affirmative Consent executed by the minor's parent or legal guardian.

- Updates to Appendices A and B reflecting the approval of the new Level 1 Multi Provider Consent Form, the Level 1 Payer Consent Form, and the Level 2 Payer Consent for Payment Consent Form

The scope of the RHIO Privacy and Security Policies and Procedures – V1.1 includes the full range of privacy and security policies for interoperable health information exchange, including: authorization, authentication, consent, access, audit, breach and patient engagement policies.

The New York State Department of Health ("NYS DOH") has participated in developing the RHIO Privacy and Security Policies and Procedures – V1.1. It is the opinion of the NYS DOH that the RHIO Privacy and Security Policies and Procedures – V1.1 are compliant with state and federal laws.

The RHIO Privacy and Security Policies and Procedures – V1.1 were developed as part of a Statewide Collaboration Process ("SCP"), the participants in which include all recipients of grant funding under Phase 5 of the Health Care Efficiency and Affordability Law for New Yorkers Capital Grant Program ("HEAL 5") and other interested stakeholders in the health care system of New York State.

The Policies and Procedures are components of a larger State effort to advance the development of the SHIN-NY. The SHIN-NY is conceived of as a "network of networks" designed to enable patient health information to be exchanged in real time among disparate clinicians, other authorized entities and patients, while ensuring security, privacy and other protections. The purpose of the SHIN-NY is to provide the technological underpinning so that:

- Clinical information is in the hands of clinicians to guide medical decisions and improve care coordination;

- Medical information follows the consumer so they are at the center of their care;

- Quality initiatives result in robust accountability based on the information needed to assess patient outcomes;

- Clinical information is accurately collected in a timely manner for population health reporting, clinical trials and other research purposes; and

- Clinical research and care delivery are linked together to measure and monitor longitudinal outcomes.

The SHIN-NY is intended to support New York's health care transformation agenda, including efforts to improve health care quality, affordability and outcomes.

The Role of RHIOs

The RHIO Privacy and Security Policies and Procedures – V1.1 apply only to health information exchange that occurs as part of the SHIN-NY and is governed by the New York eHealth Collaborative ("NYeC"), RHIOs or similar entities designated by the State. A RHIO is a not-for-profit corporation that (i) receives funding under and was designated as a RHIO under Phase 5 of the Healthcare Efficiency and Affordability Law for New Yorkers or (ii) is otherwise designated as a RHIO by the NYS DOH or (iii) meets the definition of a RHIO as set forth in the HEAL 5 Request for Grant Applications and agrees in writing with NYeC to follow the Statewide Policy Guidance applicable to RHIOs as developed through the SCP.

RHIOs are comprised of health care organizations whose mission is to govern the SHIN-NY in the public's interest and ensure all providers in a defined region are participating in and connected to the SHIN-NY. RHIOs are contractually required by the State of New York to participate in the SCP and to comply with the Statewide Policy Guidance that is developed through that process. The development of, and compliance with, the Statewide Policy Guidance is essential to ensuring adherence to information policies and procedures, standards and technical approaches that enable the secure and interoperable exchange of health information—one of the principal goals of the SHIN-NY and the key to realizing the potential benefits of public investment in health information technology ("health IT") infrastructure.

The Statewide Collaboration Process

At the present time, New York State has elected to develop Statewide Policy Guidance through the SCP, rather than through legislative or regulatory mandates. The SCP is being facilitated by NYeC under contract with the NYS DOH. NYeC is a public-private partnership and statewide governance body playing an integral role in the development of policies through a multi-stakeholder, consensus-based approach as part of New York's health IT strategy. NYeC's key responsibilities include (1) convening, educating and engaging key constituencies, including health care and health IT leaders across the state, RHIOs, Community Health Information Technology Adoption Collaboratives ("CHITAs"), and other health IT initiatives; (2) developing Statewide Policy Guidance through a transparent governance process, and (3) evaluating and establishing accountability measures for New York's health IT strategy.

The SCP is designed to collaboratively develop common policies and procedures, standards, technical approaches and services for New York's health information infrastructure. Participants include representatives of all the health IT projects receiving funding under HEAL 5 and other interested stakeholders in the health care system of New York State. Within the SCP decisions are made and recommendations advanced in a collaborative, consensus-based manner through a fully open, transparent process. The SCP is largely driven by the efforts of its four collaborative work groups, which recommend policies and procedures, standards, technical approaches and services initially to the NYeC Policy and Operations Council, and thereafter to the NYeC Board and NYS DOH. The four work groups are: (1) Clinical Priorities; (2) Privacy and Security; (3) Protocols and Services; and (4) EHR Collaborative.

The Statewide Collaboration Process: Policies and Procedures

The SCP provides a framework where developing policies and standards for New York's health information infrastructure go hand in hand with field testing them as part of HEAL 5 projects' implementations. This framework allows for the validation and ongoing refinement of policies and standards to ensure health information liquidity and value realization. This is a crucial process over the next few years.

Process for Development of RHIO Privacy and Security Policies and Procedures – V1.1

The RHIO Privacy and Security Policies and Procedures – V1.1 are the product of a long-standing development process that began in 2006 with the Health Information Security and Privacy Collaboration ("HISPC"), a national initiative that was funded by the federal Office of the National Coordinator for Health IT and Agency for Healthcare Research and Quality. HISPC was designed to examine how privacy and security laws impact business practices related to electronic health information exchange.

The HISPC project consisted of two phases. Phase I spanned from March 2006 to April 2007 and involved a comprehensive assessment of health privacy legal and policy issues in New York. A central finding of Phase I of HISPC was that strong policies that protect the privacy and security of health information are crucial to achieving interoperable health information exchange and that the electronic exchange of health information through the state demands new approaches for protecting privacy and security, including policies addressing the disclosure and use of health care information, and technologies that address consumer identification, authentication, record location, identity management, and storage of special classes of information.

The NY HISPC Phase I project advanced an "Implementation Framework." One of the four priority solution areas was consumer consent – ensuring that consumers are able to provide informed and meaningful consent and that holders of health information adhere to state and federal privacy and security laws as they exchange health information electronically.

The second phase of NY HISPC began in July 2007. This phase focused on the development of a consumer consent solution through a standardized consent process that would be part of a comprehensive set of health information privacy and security policies. The goal of this standardized process was to promote consistency across New York State RHIOs in obtaining consent and addressing consumer privacy concerns about electronic exchange of health information.

To engage in a statewide dialogue on consent, four stakeholder meetings were held in September 2007, October 2007 and March 2008 to identify consent-related issues and to gain consensus on a standardized approach. The meetings were attended by consumer advocates, health care providers, RHIO executive and clinical leaders, representatives from the New York City Department of Health, and others. The first meeting was dedicated to understanding the current state of RHIO policy development regarding consumer consent. The second meeting sought to elicit discussion on the key policy questions that a new consent policy for RHIOs would need to address. At the third meeting, "straw model" recommendations were proposed and discussed. At the fourth and final meeting, an analysis of the "straw model" recommendations was presented and discussed in the form of developed policy recommendations. These privacy and security recommendations were documented in a White Paper entitled "Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York State" (the "Privacy and Security White Paper"), which was subject to public comment in March 2008 through a process overseen by NYS DOH.

Following the public comment period on the Privacy and Security White Paper, the Privacy and Security Work Group of the SCP was formed. It is charged with the development of Statewide Policy Guidance to protect privacy, strengthen security, ensure affirmative and informed consent, and support the right of New Yorkers to have greater control over and access to their Protected Health Information as foundational requirements for interoperable health information exchange. Over a period of six months from June to

The Statewide Collaboration Process: Policies and Procedures

November, 2008, the Privacy and Security Work Group further refined the recommendations set forth in the Privacy and Security White Paper by specifically addressing a number of issues that were identified through the public comment period as requiring further analysis. Based on the review of broad and sometimes conflicting sets of comments from Work Group members, the Privacy and Security Work Group revised the Privacy and Security White Paper and developed the RHIO Privacy and Security Policies and Procedures – V1.0 and V1.1 for consent, authorization, access, authentication, audit, breach and patient engagement.

Who Must Comply with the RHIO Privacy and Security Policies and Procedures – V1.1

All projects funded as RHIOs under the HEAL NY Phase 5 Health IT grant program or otherwise recognized as RHIOs by the NYS DOH are required to comply with the RHIO Privacy and Security Policies and Procedures – V1.1. In addition, all RHIOs must require their Participants to comply with the RHIO Privacy and Security Policies and Procedures – V1.1. CHITAs, which are informal collaborations of health care providers that are recipients of funding under Phase 5 of HEAL-NY, are not legal entities, but their participants will also be required to comply with the RHIO Privacy and Security Policies and Procedures – V1.1 when exchanging health information through the SHIN-NY governed by a RHIO.

The RHIO Privacy and Security Policies and Procedures – V1.1 represent the *minimum* standards with which RHIOs must comply and must require their Participants to satisfy. Where appropriate, or where required by the operational models and/or governance structures of the RHIO, a RHIO may delegate certain of the responsibilities set forth in the RHIO Privacy and Security Policies and Procedures – V1.1 to its Participants. However, RHIOs remain responsible for requiring their Participants to comply with the minimum policies set forth herein.

These Policies and Procedures apply to information exchanged via the SHIN-NY governed by a RHIO, as defined herein. In order to avoid significant unintended consequences that could impact a range of electronic health information activities that are adequately regulated and do not constitute community-wide or statewide health information exchange, One-to-One Exchanges, including those conducted via the SHIN-NY governed by a RHIO, are excluded from the requirements set forth in these Policies and Procedures. While One-to-One Exchanges are excluded from the requirements in the Policies and Procedures, they remain subject to all applicable federal and state laws.

Process for Amendment to RHIO Privacy and Security Policies and Procedures – V1.1

Beginning in the first half of 2009, and on an ongoing basis thereafter, an operational guide to assist RHIOs and their Participants in implementing these RHIO Privacy and Security Policies and Procedures – V1.1 will be developed through the SCP. It is anticipated that learning more about the operational ramifications of these RHIO Privacy and Security Policies and Procedures – V1.1 will lead to a need to revise and refine the Policies and Procedures to reflect what is learned. All future versions of the Policies and Procedures will be developed, reviewed and approved through the SCP.

Definitions:

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 Form; (ii) a Level 2 Consent Form; (iii) a consent form approved by NYS DOH as an alternative to

a Level 1 Consent Form or a Level 2 Consent Form under Section 1.4; or (iv) a consent form that may be relied upon under the Patient Consent Transition Rules set forth in Section 1.8.2.

Approved Consent Form means an Affirmative Consent other than a consent form relied upon by a Participant under the Patient Consent Transition Rules set forth in Section 1.8.2.

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

Authorized User means an individual who has been authorized by a Participant or a RHIO to access patient information via the SHIN-NY governed by a RHIO in accordance with the RHIO Privacy and Security Policies and Procedures – V1.1.

Breach means any unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of Protected Health Information or Demographic Information. An Incidental Disclosure by a RHIO or one of its Participants is not a Breach.

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 1.2.3.

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.

Consent Implementation Date means the date by which the NYS DOH requires RHIOs to begin to utilize an Approved Consent Form. In establishing such date, NYS DOH shall take into account the time that will be required for individual RHIOs to come into compliance with the policies and procedures regarding consent set forth herein.

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

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

Incidental Disclosure means a secondary use or disclosure that (i) cannot reasonably be prevented; (ii) is limited to Demographic Information other than any elements of a social security number except the last four digits thereof[1]; (iii) occurs as a by-product of an otherwise permitted use or disclosure; and (iv) occurs notwithstanding the implementation by the RHIO and/or its Participants of reasonable safeguards to limit disclosures, consistent with these RHIO Privacy and Security Policies and Procedures-V1.1.

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 Form means a consent in the form attached hereto as Appendix A.

Level 2 Consent Form means a consent 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.

Marketing means (1) any communication about a product or service that encourages recipients to purchase or use the product or service, unless the communication is made (i) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; (ii) for the treatment of the individual; or (iii) for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; or (2) an arrangement whereby a Participant discloses Protected Health Information to another entity, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services.

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 for certain types of health services (e.g., family planning, HIV testing, mental health or substance abuse treatment).

NYS DOH means the New York State Department of Health.

New York eHealth Collaborative ("NYeC") means the New York not-for-profit corporation organized for the purpose of (1) convening, educating and engaging key constituencies, including health care and health IT leaders across New York State, RHIOs, CHITAs and other health IT initiatives; (2) developing common health IT policies and procedures, standards, technical requirements and service requirements through a transparent governance process and (3) evaluating and establishing accountability measures for New York State's health IT strategy. NYeC is under contract to the NYS DOH to administer the SCP and through it develop Statewide Policy Guidance.

One-to-One Exchange means a disclosure of Protected Health Information by one of the patient's providers to one or more other providers treating the patient with the patient's knowledge and implicit or

[1] Note that inclusion of the last four digits of a social security number is pending DOH Legal approval.

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 or lab results sent to the Practitioner who ordered them.

Participant means a Provider Organization, Payer Organization, or Practitioner that has directly or indirectly entered into a Participation Agreement with a RHIO and accesses Protected Health Information via the SHIN-NY governed by a RHIO.

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

Patient Consent Transition Rules means the rules set forth in Section 1.8.

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 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.

Privacy and Security White Paper means the final draft of the policy paper, as approved by each of the NYeC Board of Directors and the NYS DOH, entitled "Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York State."

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 in New York State.

Quality Improvement means conducting quality measurement, assessment and improvement, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health and reducing health care costs, evaluating Practitioner and provider performance, clinical decision support tools, evidence-based clinical protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives and related functions. Care management by payers may include (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; provided, however, that no such activity may include utilization review or other tasks designed to determine whether a payer should cover or make payment for a health care service.

Record Locator Service or Other Comparable Directory means a system, queriable 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.

RHIO means a not-for-profit corporation that (i) receives funding and was designated as a RHIO under Phase 5 of the Healthcare Efficiency and Affordability Law for New Yorkers or (ii) is otherwise designated as a RHIO by the NYS DOH or (iii) an organization that meets the definition of RHIO as set forth in the HEAL 5 Request for Grant Applications and agrees in writing with NYeC to follow the Statewide Policy Guidance applicable to RHIOs as developed through the SCP.

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 "network of networks" overseen by NYS DOH and governed by RHIOs, which enables patient health information to be exchanged in real time among disparate clinicians, other authorized entities, and patients, while ensuring security, privacy and other protections.

Statewide Collaborative Process ("SCP") means the open, transparent process to which multiple stakeholders contribute, administered by NYeC, to develop Statewide Policy Guidance, to be adopted and complied with by all RHIOs and their Participants.

Statewide Policy Guidance means the common policies and procedures, standards, technical requirements and service requirements developed through the SCP.

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.

The Statewide Collaboration Process: Policies and Procedures

SECTION 1: CONSENT

Purpose/Principles

The purpose of these Policies and Procedures is to ensure the privacy and security of patients' Protected Health Information while facilitating the sharing of such information to provide better quality health care.

Current laws governing health information exchange and the resulting business practices were developed in the context of a paper-based health care environment where decisions regarding what, how and to whom to communicate were generally made on a one-to-one basis by clinicians. Current laws attempt to serve patients' privacy interests by restricting what can and cannot be shared, and the terms on which sharing takes place. Human judgment and personal relationships play a major role, as clinicians attempt to act as guardians of their patients' information.

Moving from a paper to an electronic health system changes the information-sharing dynamic. An interoperable health system facilitates a many-to-many relationship, enabling different information technology systems and software applications to exchange information accurately, effectively and consistently. This offers new opportunities to promote patient access to and control over health care information, as well as to facilitate the safety, quality and efficiency of health care.

Requiring patients to consent to the exchange of their information via the SHIN-NY governed by a RHIO ensures that they know how their information will be shared and used among RHIO Participants. It also lets patients decide whether to allow their information to be shared and used in this manner. The Policies and Procedures set forth in this Section 1 prescribe minimum State requirements for obtaining patient consent to exchange health information via the SHIN-NY governed by a RHIO.

Patient consent is an important element in achieving informed and trusted interoperable health information exchange as well as satisfying New York laws and regulations. It is important to observe, however, that consent policies alone are not enough and that such policies must be accompanied by privacy and security protections relating to authorization, authentication, access, audit and enforcement to earn consumer trust and enable successful health information exchange. Furthermore, it is essential that patient consent be implemented in conjunction with a robust consumer education program to ensure the consent decision is well informed.

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 RHIO 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 1.7.5.

1.2 **Exceptions to Affirmative Consent Requirement.** Notwithstanding anything to the contrary set forth in this Section 1, 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 RHIO from another Participant that is treating the patient 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.[2]

1.2.2 Public Health Reporting. If a Data Supplier is permitted to disclose Protected Health Information to a government agency for purposes of public health reporting without patient consent under applicable State and federal laws and regulations, a RHIO may make that disclosure on behalf of the Data Supplier without Affirmative Consent.

1.2.3 Breaking the Glass When Treating a Patient with an Emergency Condition.

a. Affirmative Consent shall not be required for a Practitioner to access Patient Health Information via the SHIN-NY governed by a RHIO and the Practitioner may Break the Glass if the following conditions are met:

i. Treatment may be provided to the patient without informed consent as provided in Public Health Law Section 2504(4), i.e., in the Practitioner'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 determines, in his or her reasonable judgment, that information that may be held by or accessible via the SHIN-NY governed by a RHIO 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 is affiliated.

iv. The Practitioner attests that all of the foregoing conditions have been satisfied, and the RHIO software maintains a record of this access.

b. RHIOs shall ensure, or shall require their Participants to ensure, that access to information via the SHIN-NY governed by a RHIO without Affirmative Consent when treating a patient pursuant to this Section 1.2.3 terminates upon the completion of the emergency treatment.

c. Notwithstanding anything to the contrary set forth in these policies, a RHIO and its Participants shall not be required to exclude any Sensitive Health Information from access via the SHIN-NY governed by a RHIO where the circumstances set forth in this Section 1.2.3 are met.

1.2.4 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 RHIO, provided that (i) the RHIO is

[2] 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.

serving as the Data Supplier's Business Associate (as defined in 45 C.F.R. § 160.103) and (ii) the RHIO does not make the information accessible to Participants until Affirmative Consent is obtained, except as otherwise permitted herein.

1.2.5 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.

1.3 Form of Patient Consent. Except as otherwise permitted by the Patient Consent Transition Rules set forth at Section 1.8, consents shall be obtained through an Approved Consent Form. A RHIO may request approval to use a consent form other than a Level 1 Consent Form or Level 2 Consent Form if it obtains approval from NYS DOH. Such approval will not be granted unless the alternative form is substantially similar to the Level 1 Consent Form or Level 2 Consent Form, as applicable, and achieves the same basic purposes as such consent forms, as set forth in these policies.

1.3.1 Level 1 Uses. Consent to access information via the SHIN-NY governed by a RHIO for Level 1 Uses shall be obtained using a Level 1 Consent Form or an alternative form approved by NYS DOH 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, substance abuse and genetic 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 RHIO website or other means; the consent form shall also identify whether the RHIO is party to data sharing agreements with other RHIOs and, if so, provide instructions for patients to access an up-to-date list of Data Suppliers from a RHIO 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 RHIO for the purposes of Level 2 Uses shall be obtained using a Level 2 Consent Form or an

alternative form approved by NYS DOH 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 RHIO 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 Forms. Consent for Level 1 Uses and consent for Level 2 Uses shall not be combined into one form.

1.4 Sensitive Health Information.

1.4.1 General. An Affirmative Consent may authorize the Participant(s) listed on the consent form to access all Protected Health Information referenced on the consent form, including Sensitive Health Information.[3]

1.4.2 Withholding Sensitive Health Information. RHIOs 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 RHIO. In the event that a RHIO 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 RHIO, and the patient has exercised that option, the patient's record when accessed via the SHIN-NY governed by a RHIO may, but is not required to, carry an alert indicating that data has been withheld from the record.

1.4.3 Re-disclosure of Sensitive Health Information. 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 said information, including those applicable to HIV/AIDS and alcohol and substance abuse information.

1.5 Special Provisions Relating to Minors.

1.5.1 Exchange of Information for Minors under Ten Years of Age. RHIOs and their Participants may permit the exchange of information about minors below ten years of age based on an Affirmative Consent executed by the minor's parent or legal guardian.

---

[3] The disclosure of records of federally-assisted alcohol and drug abuse programs is governed by federal regulations. 42 C.F.R. Part 2. While the State believes that policies set forth herein, including use of the Approved Patient Consent Form, are consistent with the regulations' consent requirements, the State does not have authority to interpret these regulations. SAMHSA, which is vested with such authority, has not yet provided clear guidance on this issue. Thus, RHIOs must individually assess the legal risk of exchanging substance abuse treatment information based on the affirmative consent policies set forth herein.

1.5.2 Exchange of Minor Consent Information for Minors Ten Years of Age or Older.

a. RHIOs and their Participants shall permit the exchange of Minor Consent Information about minors ten years of age or older only when the minor has given consent to such exchange.

b. RHIOs shall require Participants to obtain a minor's consent to exchange Minor Consent Information at the time the services to which the minor is granting consent are provided.

c. Notwithstanding the foregoing, a RHIO may permit the exchange of Protected Health Information about a minor without the minor's consent in accordance with Section 1.2.3 when treating a minor with an emergency condition.

1.5.3 Emancipated Minors. Participants may rely on the Affirmative Consent of an emancipated minor to the access of Protected Health Information of such minor via the SHIN-NY governed by a RHIO. Participants may also rely on a consent previously granted by the parent of a now-emancipated minor; provided that once the minor reaches the age of majority, no further access to the minor's Protected Health Information shall be permitted until the minor executes a new Affirmative Consent.

1.6 De-Identified Data.

1.6.1 Access of De-Identified Data for Specified Uses. Affirmative Consent shall not be required for a Participant to access De-Identified Data via the SHIN-NY governed by a RHIO for the following purposes:

a. Research approved by an Institutional Review Board or Privacy Board organized and operating in accordance with 45 C.F.R. § 164;

b. Public health purposes, in accordance with 45 C.F.R § 164.512(b),or as authorized by other federal and state laws or regulations, 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; and

c. Evaluation and improvement of RHIO operations, including analyses performed by the RHIO, government agencies or their contractors.

1.6.2 Other Requirements.

a. All other uses of De-Identified Data shall require Affirmative Consent.

b. A RHIO shall not condition a patient's participation in the RHIO 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. RHIOs 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. RHIOs shall, or shall require Participants to, subject any use of De-Identified Data to adequate restrictions on the re-identification of said data.

1.7 Other Policies and Procedures Related to Consent.

1.7.1 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.

1.7.2 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.

1.7.3 Consent Forms Covering Multiple Participants. An Affirmative Consent may apply to more than one Participant provided that the consent form (i) lists each Participant with sufficient specificity to provide reasonable notice to the patient as to which Participant may access the patient's information via the SHIN-NY governed by a RHIO pursuant to such consent form and (ii) provides the patient with the option to select which of the Participants listed on the consent form may access the patient's information via the SHIN-NY governed by a RHIO. Any Participant accessing information based on a consent form covering multiple Participants must be identified on such consent form at the time the patient grants Affirmative Consent.

1.7.4 Consent Obtained by RHIOs. RHIOs 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.

1.7.5 Electronic Signatures. Affirmative Consent may be obtained electronically provided that there is an electronic signature that meets the requirements of the federal ESIGN statute, 15 U.S.C. § 7001 *et seq.*, or any other applicable New York State or federal laws or regulations.

1.7.6 Denial of Consent. Consent forms shall give the patient the option of granting or affirmatively denying consent for Participants to access information about the patient via the SHIN-NY governed by a RHIO. A patient's decision not to sign a consent form shall not be construed as a "denial of consent" under Section 1.2.3(a)(iii).

1.7.7 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 Form is executed, except to the extent a longer duration is required to complete a research protocol.

1.7.8 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 RHIO prior to such revocation and incorporated such Protected Health Information into its records from retaining such information in its records.

1.7.9 Notification of a RHIO's Data Suppliers. RHIOs shall provide, or shall require their Participants to provide, patients with a list of or reference to all Data Suppliers at the time the RHIO or Participant obtains the patient's Affirmative Consent. Each RHIO shall provide convenient access at all times thereafter, either through its website or otherwise, to a complete and accurate updated list of Data Suppliers.

1.7.10 Compliance with Business Associate Agreements with Data Suppliers. A RHIO shall not use or disclose Protected Health Information in any manner that violates the RHIO's Business Associate Agreements with Data Suppliers.

1.7.11 Disclosure to Vendors. A RHIO, 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 RHIO's authorized activities provided (i) the RHIO requires the vendors to protect the confidentiality of the Protected Health Information in accordance with the RHIO'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.

1.7.12 Compliance with Existing Law. All access to Protected Health Information via the SHIN-NY governed by a RHIO 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 Patient Consent Transition Rules.

1.8.1 Use of Approved Consent Form. Except as set forth in Section 1.8.2, each RHIO shall be required to utilize an Approved Consent Form with respect to all patients who consent to the exchange of Protected Health Information via the SHIN-NY governed by a RHIO *on or after* the Consent Implementation Date.

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

1.8.3 Use of Existing Consent Form After Consent Implementation Date. A RHIO may continue to use an Existing Consent Form after the Consent Implementation Date if the Existing Consent Form is approved by NYS DOH under Section 1.3.

The Statewide Collaboration Process: Policies and Procedures

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 RHIO. 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. This Section 2 sets forth minimum requirements that RHIOs 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 RHIO. They are designed to limit exchange of information to the minimum 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 RHIO.

Policies and Procedures

2.1 Role-Based Access Standards.

2.1.1 RHIOs 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 RHIO; 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 RHIO 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, RHIOs 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. Practitioner with access to clinical information and Break the Glass authority;

b. Practitioner with access to clinical information but no Break the Glass authority;

c. Non-Practitioner with access to clinical information;

d. Non-Practitioner with access to non-clinical information;

e. RHIO administrators with access to non-clinical information; and

f. RHIO administrators with access to clinical information in order to engage in public health reporting purposes in accordance with Section 1.2.2 of these Policies.

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

The Statewide Collaboration Process: Policies and Procedures

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 RHIO is who he or she claims to be. This is accomplished by providing proof of identity. This Section 3 sets forth minimum requirements that RHIOs and their Participants shall follow when authenticating individuals prior to allowing them to access information via the SHIN-NY governed by a RHIO. 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. RHIOs 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 RHIO. Such authentication shall take place in accordance with the provisions of this Section 3.

3.2 Authentication Requirements.

3.2.1 Transitional Authentication Standard. Until such time as a determination is made, pursuant to Section 3.2.2, to utilize a higher authentication standard, RHIOs shall authenticate, or shall require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Authentication Assurance Level 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, RHIOs 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, RHIOs 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 RHIOs 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 RHIO.

3.2.2 Minimum 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 Authentication Assurance Level 3 ("Level 3") set forth in NIST SP 800-63, RHIOs shall be required to authenticate, or require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Level 3. NYeC shall, through the SCP, establish a Work Group to 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.

a. Level 3 will require, among other technical specifications, RHIOs 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). RHIOs 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 RHIOs 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 RHIO, 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, RHIOs 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, RHIOs may utilize such statewide services to authenticate an Authorized User in accordance with the provisions of this Section 3.

The Statewide Collaboration Process: Policies and Procedures

SECTION 4: ACCESS

Purpose/Principles

Access controls govern when and how a patient's information may be accessed by individuals within a RHIO's Participant. This Section 4 sets forth minimum behavioral controls RHIOs shall implement to ensure that: 1.) only Authorized Users access information via the SHIN-NY governed by a RHIO; 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.** RHIOs shall, or shall require their Participants to, ensure that each Authorized User is assigned a unique user name and password to provide such Authorized User with access to patient information via the SHIN-NY governed by a RHIO. In doing so, RHIOs 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 and/or passwords with others and from using the user names and/or passwords of others.

4.2 **Authorized Purposes.** RHIOs and their Participants shall permit Authorized Users to access Protected Health Information of a patient via the SHIN-NY governed by a RHIO only for purposes consistent with a patient's Affirmative Consent.

4.3 **Failed Access Attempts.** RHIOs shall enforce a limit of consecutive Failed Access Attempts by an Authorized User. Upon a fifth Failed Access Attempt, RHIOs shall ensure that said Authorized User's access to the RHIO is disabled either by locking the account until release by a RHIO administrator or by locking the account for a specific period of time as specified by the RHIO, after which the Authorized User may reestablish access using appropriate identification and authentication procedures.

4.4 **Periods of Inactivity.** RHIOs shall ensure that an Authorized User is automatically logged out of the RHIO 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. RHIOs 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.** RHIOs 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 RHIO 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, RHIOs shall, or shall require their Participants to:

4.6.1 Implement reasonable safeguards to minimize Incidental Disclosures during the process of identifying a patient and locating a patient's medical records.

4.6.2 Prohibit Authorized Users from accessing Protected Health Information in any manner inconsistent with these Policies and Procedures - V1.1.

4.7 **Training.** The behavioral and organizational access controls set forth above will only be effective if 1) a RHIO'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, RHIOs shall develop and 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 RHIO.

4.7.1 RHIOs 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 RHIO and the policies and procedures governing access to information via the SHIN-NY governed by a RHIO.

4.7.2 RHIOs 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 RHIO.

4.7.3 RHIOs 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 RHIO's policies and procedures. Such certification shall be retained by RHIOs or their Participants for at least six years.

4.7.4 RHIOs may, but shall not be required to, ensure that each Authorized User undergo continuing and/or refresher training on a periodic basis as a condition of maintaining authorization to access patient information via the SHIN-NY governed by a RHIO.

4.8 **Termination of Access and Other Sanctions.** RHIOs 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 RHIOs shall ensure that access to the RHIO of a Participant (and all of the Participant's Authorized Users, if applicable) is terminated in the following situations and in accordance with the processes described:

a. 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 RHIO; and/or

b. Immediately or as promptly as reasonably practicable but in any event within one business day of notification of termination of an Authorized User's employment or affiliation with the Participant.

4.8.2 In order to comply with Section 4.8.1(b), RHIOs shall require their Participants to notify the RHIO upon of termination of an Authorized User's employment or affiliation with the Participant immediately or as promptly as reasonably practicable but in any event within one business day of termination.

4.8.3 RHIOs shall establish sanctions to redress policy or procedural violations. Sanctions could include temporary access prohibitions, re-training requirements, termination, or other processes the RHIO deems necessary in accordance with its internal risk analyses.

4.8.4 The SCP shall develop guidance on the following to be included in V2.0 of these Policies and Procedures: 1.) How RHIOs should respond to discovery requests and subpoenas; 2.) Whether state-level sanctions should be developed and implemented by RHIOs.

The Statewide Collaboration Process: Policies and Procedures

SECTION 5: PATIENT ENGAGEMENT AND ACCESS

Purpose/Principles

RHIOs present an opportunity for patients to gain access to their health information through a single electronic portal, thereby eliminating many of the bureaucratic hurdles patients currently endure when attempting to obtain copies of their medical records. Openness about policies, procedures, technology, and practices among Participants exchanging health information via the SHIN-NY governed by a RHIO is a foundational principle essential to protecting patient privacy and to realizing the potential for RHIOs to markedly improve patient access to their own health information. This Section 5 sets forth minimum requirement RHIOs and their Participants shall follow to ensure that patients are able to understand what information exists about them, how that information is used, and whether and how they can access such information.

Policies and Procedures

5.1 RHIOs shall be required to educate patients 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.

5.2 RHIOs shall, or shall require their Participants to, develop and educate patients with respect to policies related to patients' rights to access their own Protected Health Information. RHIOs are not required to provide patients with access to their own Protected Health Information, but they are encouraged to do so and are required to inform patients as to whether such access is available to them.

5.3 To facilitate informed consent and to ensure that patients know where information about them is being generated, RHIOs shall provide, or shall require their Participants to provide, patients with a list of or reference to all Data Suppliers (consistent with Section 1.7.9) and information about how to contact said Data Suppliers.

5.4 If patient access to Protected Health Information is provided by a RHIO, the RHIO shall inform the patient as to all material terms and conditions relating to such access. Patient access 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. For example, patient access must be in accordance with federal and state laws regarding denial of access to medical information if, in the exercise of professional judgment, a licensed health care professional believes that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.

5.5 Each RHIO shall develop a plan and process for assuring meaningful patient/consumer input and participation in RHIO operations and decision making. Each RHIO 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 RHIO policies and procedures. At a minimum, each RHIO shall appoint at least one patient representative to its Board of Directors. A patient representative is defined as a person whose interest in the RHIO is as a patient or representative of patients and who does not otherwise participate in or have a financial interest in the RHIO or one of its Participants.

The Statewide Collaboration Process: Policies and Procedures

[Note: The SCP's Consumer Advisory Council will consider whether additional patient/consumer education policies should be included in future versions of the Policies and Procedures.]

The Statewide Collaboration Process: Policies and Procedures

SECTION 6: AUDIT

Purpose/Principles

Audits are useful oversight tools for recording and examining access to information through a RHIO (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 RHIOs and their Participants shall follow when logging and auditing access to health information via the SHIN-NY governed by a RHIO.

Policies and Procedures

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

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.

6.1.2 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.

6.1.3 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 RHIO shall conduct, or shall require each of its Participants to conduct, periodic audits to monitor use of the RHIO by Participants and their Authorized Users and ensure compliance with Policies and Procedures and all applicable laws, rules and regulations.

6.2.1 At a minimum, the RHIO 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 RHIO, other than in Break the Glass situations;

b. That Authorized Users who access Protected Health Information via the SHIN-NY governed by a RHIO do so for Authorized Purposes; and

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

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

6.2.3 Periodic audits shall be conducted at least on an annual basis. RHIOs shall consider their own risk analyses and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine the reasonable and appropriate frequency with which to conduct audits more often than annually.

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

6.2.5 If audits are conducted by Participants rather than by the RHIO, the RHIO shall:

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

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

6.3 Participant Access to Audit Logs.

6.3.1 A RHIO 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 RHIO:

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 RHIOs 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 RHIO shall, or shall require its Participants to, provide patients, upon request, with the following information:

a. The name and role (e.g., physician) of each Authorized User who accessed a patient's Protected Health Information in the prior 6-year period;

b. The Participant through which such Authorized User accessed such Protected Health Information;

c. The time and date of such access; and

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

6.4.2 RHIOs shall, or shall require their Participants to provide such information as promptly as reasonably practicable but in no event more than ten calendar days after receipt of the request.

6.4.3 If requested, RHIOs shall, or shall require their Participants to, provide such information to patients at no cost once in every 12-month period. RHIOs may establish a reasonable fee for any additional requests within a given 12-month period; provided that the RHIO shall waive any such fee where such additional request is based on a reasonable suspicion of unauthorized access to the patient's Protected Health Information via the SHIN-NY governed by a RHIO.

6.4.4 If applicable, RHIOs shall, or shall require their Participants to, provide notice of the availability of such information on any patient portals maintained by the RHIO or its Participants.

6.5 Public Availability of Audits. Each RHIO shall make the results of its periodic audit available on the RHIO'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.

[Note: Work Group agreed to consider inclusion of a search audit requirement in future versions of the Policies and Procedures.]

The Statewide Collaboration Process: Policies and Procedures

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 RHIOs and their Participants are not held accountable and to certain behavioral standards when privacy violations occur. This Section 7 sets forth minimum standards RHIOs and their Participants shall follow in the event of a breach. They are designed to hold violators accountable for violations, assure patients about the RHIO'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 RHIO shall require its Participants to notify the RHIO in the event that a Participant becomes aware of any actual or suspected Breach of Protected Health Information accessed via the SHIN-NY governed by a RHIO.

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 RHIO.** RHIOs shall be required to develop a Breach plan as part of their policies and procedures. The plan shall provide that, in the event a RHIO becomes aware of any actual or suspected Breach, either through notification by a Participant or otherwise, the RHIO must, at a minimum:

7.2.1 Notify any Participants whose data is affected by the Breach.

7.2.2 In the most expedient time possible and without unreasonable delay, investigate (or require the applicable Participant to investigate) the scope and magnitude of such actual or suspected Breach, and identify the root cause of the Breach.

7.2.3 Mitigate (or require the applicable Participant to mitigate) to the extent practicable, any harmful effect of such Breach that is known to the RHIO or the Participant. RHIOs' mitigation efforts shall correspond with and be dependent upon their internal risk analyses.

7.2.4 Notify (or require the applicable Participant to notify) the patient and any applicable regulatory agencies as required by applicable federal, state and local laws and regulations, except if a law enforcement agency determines that such notification impedes a criminal investigation.

7.3 **Sanctions.** Each RHIO shall establish appropriate sanctions that shall apply to Participants and their authorized Users in the event of a Breach of these policies and procedures and shall apply, or require its Participants to apply, such sanctions. Such sanctions may include but shall not be limited to temporarily restricting an Authorized User's access to the RHIO; requiring Authorized Users to undergo additional training in the use of the RHIO; terminating the access of an Authorized User to the RHIO; terminating a Participant's participation in the RHIO; or such other remedies as the RHIO may reasonably deem necessary in accordance with its internal risk analysis."

The Statewide Collaboration Process: Policies and Procedures

APPENDIX A: MODEL LEVEL 1 CONSENT FORMS

See approved Level 1 Single Provider Consent Form, Level 1 Multi-Provider Consent Form, and Level 1 Payer Consent Form available on the NYeC website at http://www.nyehealth.org/SCP-policies.

The Statewide Collaboration Process: Policies and Procedures

APPENDIX B: MODEL LEVEL 2 CONSENT FORMS

See approved model Level 2 Payer Consent Form for Payment available on the NYeC website at http://www.nyehealth.org/SCP-policies.

80446675.5