HEALTHIX

PRIVACY AND SECURITY POLICIES AND PROCEDURES

Introduction

These Policies and Procedures provide a common and consistent framework for the exchange of patient health information through Healthix.

Definitions:

42 CFR Part 2 means Federal regulations governing the confidentiality of drug and alcohol abuse treatment and prevention records. The regulations set forth requirements applicable to certain federally assisted substance abuse treatment programs limiting the use and disclosure of substance abuse patient records and identifying information. These regulations were enacted in 1987 by the Secretary of the US Department of Health and Human Services (HHS) as authorized by both the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970 and the Drug Abuse Prevention, Treatment, and Rehabilitation Act of 1972. These Acts and the Part 2 regulations provide comprehensive privacy protections in an effort to encourage people to seek treatment for substance abuse problems. Part 2 sets forth the limited circumstances in which substance abuse patient information may be used or disclosed, and no uses or disclosures other than those detailed in the regulations are permitted.

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

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

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

Affirmative Consent means the consent of a patient obtained through the patient's execution of (i) a Level 1 Consent; (ii) a Level 2 Consent; (iii) an Alternative Consent; or (iv) a consent that may be relied upon under the Patient Consent Transition Rules set forth in Section 1.8.2.

Agent means an entity or individual that acts on behalf of a Participant for purposes of Treatment, Care Management and/or Quality Improvement and requires access to Protected Health Information in order to fulfill these responsibilities. If required by HIPAA, an Agent must be a Business Associate of the Participant and have a written Business Associate Agreement with the Participant.

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

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

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

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

Authorized User means an individual who has been authorized by a Participant or Healthix to access patient information through SHIN-NY governed by Healthix in accordance with the 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 Healthix 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; (ii) 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 Healthix 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 Healthix or Participant to another person authorized to access Protected Health Information at Healthix 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 Healthix 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 1.2.3.

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, (iv) supporting a patient in following a plan of medical care or (v) assisting a patient in obtaining social services or providing social services to a patient.. 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.

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

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

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

Consent Implementation Date means the date by which the NYS DOH requires QEs to begin to utilize an Approved Consent.

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

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

Data Supplier means an individual or entity that supplies Protected Health Information to or through Healthix. Data Suppliers include both Participants and entities that supply but do not access Protected Health Information via Healthix (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 (i) satisfies the requirements of 45 C.F.R. §

164.514(b) and (ii) does not contain DNA variation information derived from sequencing, genotyping or other such technologies.

Demographic Information means a patient's name, gender, address, date of birth, social security number, and other personally identifiable information, but shall not include any information regarding a patient's health or medical treatment or the names of any Data Suppliers that maintain medical records about such patient.

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

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

EHR Incentive Programs means the Electronic Health Record Medicare and Medicaid Incentive Program set forth in 42 CFR 412, et seq. and 42 CFR 495, et seq.

Emancipated Minor means a minor who is emancipated on the basis of being married or in the armed services, or who is otherwise deemed emancipated under New York law or other applicable laws.

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

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

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

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

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

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

Health Oversight Agency 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, 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 authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

HIPAA means the Health Insurance Portability and Accountability Act of 1996 and it's implementing regulations as amended (including as amended by HITECH and its implementing regulations).

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).

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

Institutional Review Board means an administrative body appropriately constituted and established to protect the rights and welfare of human research subjects recruited to participate in research activities, which meets the requirements of federal and state regulations. The Institutional Review Board (IRB) is charged with the responsibility of reviewing, prior to its initiation, all research (whether funded or not) involving human participants. The IRB is concerned with protecting the welfare, rights, and privacy of human subjects. The IRB has the authority to approve, disapprove, monitor, and require modifications in all research activities that fall within its jurisdiction as specified by federal and state regulations.

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

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

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

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

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

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

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

Marketing has the meaning ascribed to this term under the HIPAA Privacy Rule.

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

Minor means an individual under the age of 18 years old.

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, testing or treatment of sexually transmitted infections, mental health or substance abuse treatment) or services consented to by an Emancipated Minor.

National Institute of Standards and Technology ("NIST") Cybersecurity Framework means the set of industry standards and best practices to help organizations manage cybersecurity risks that has been developed by the National Institute of Standards and Technology. The NIST Cybersecurity Framework uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

NYS DOH means the New York State Department of Health.

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, QEs, 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 Time Override shall have the meaning defined in section 1.5.2.d.

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

Organ Procurement Organization (OPO) means a regional, non-profit organization responsible for coordinating organ and tissue donations at a hospital that is designated by the Secretary of Health and Human Services under section 1138(b) of the Social Security Act (see also 42 C.F.R. 121).

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

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

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

Patient Care Alert means an electronic message about a development in a patient's medical care, such as an emergency room or inpatient hospital admission or discharge, a scheduled outpatient surgery or other procedure, or similar event, which is derived from information maintained by Healthix and is sent by the Healthix to subscribing recipients but does not allow the recipient to access any Protected Health Information through Healthix other than the information contained in the message. Patient Care Alerts may contain demographic information such as patient name and date of birth, the name of the Participant from which the patient received treatment, and limited information related to the patient's complaint or diagnosis but shall not include the patient's full medical record relating to the event that is the subject of the electronic message.

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

Patient Portal means an internet-accessible secure website, operated by a Patient Portal Operator, through which a patient (or his/her authorized representative) may gain access to the patient's personal health information for purposes of viewing, downloading, or transmitting the patient's personal health information. For clarification, the Patient Portal functions addressed herein do not include the ability of patients to complete forms online, communicate with providers, request prescription refills, pay bills, schedule medical appointments, or update the information presented on the portal; though the Patient Portal Operator may offer these functions through its Patient Portal as well.

Patient Portal Operator means an approved entity operating a Patient Portal. The Patient Portal Operator is responsible for the maintenance and management of the Patient Portal; including user account management, assuring appropriate authentication and access control, presentation of health information and user support. Patient Portal Operators include:

- Participants,
- QEs, or
- Third parties offering a Patient Portal to which patients subscribe.

Patient Portal Query means a request for information issued by a Patient Portal Operator to Healthix, which is initiated by the patient querying data on the Patient Portal. A QE that is a Patient Portal Operator, issues the Patient Portal Query under the Statewide Patient Record Lookup (sPRL) service with a Purpose of Use code of "REQUEST". Other classes of Patient Portal Operators will submit the request in a form and manner defined by Healthix.

Patient Portal Query Response means the data provided by Healthix to the requesting Patient Portal Operator in response to a Patient Portal Query.

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.

Performing Provider System (PPS) means an entity that has received approval from New York State Department of Health to implement projects and receive funds under New York's Delivery System Reform Incentive Payment Program (DSRIP).

Performing Provider System Centralized Entity (PPS Centralized Entity) means an entity owned or controlled by one or more PPS Partners that has been engaged by a PPS to perform Care Management, Quality Improvement or Insurance Coverage Reviews on behalf of the PPS.

Performing Provider System Lead Organization (PPS Lead Organization) means an entity that has been approved by NYSDOH and CMS to serve as a designated organization that has

assumed all responsibilities associated with a Delivery System Reform Incentive Payment (DSRIP) program per its program application and DSRIP award.

Performing Provider System Partner (PPS Partner) means a person or entity that is listed as a PPS Partner in the DSRIP network Tool maintained by the New York State Department of Health.

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. Healthix and its Participants may accept a parent or guardian a Personal Representative of a minor unless such parent or guardian has been disqualified under applicable laws, regulations or court orders.

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.

Privacy Board means a review body that meets the membership requirements of HIPAA and is established to act upon requests for a waiver or an alteration of the authorization requirements under HIPAA for uses and disclosures of Protected Health Information for a particular Research study.

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.

Provider of Minor Consented Services shall have the meaning defined in section 1.5.2.c.

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 State 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 Healthix and accesses Protected Health Information via SHIN-NY governed by Healthix.

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 with the State Designated Entity under 10 N.Y.C.R,R. Section 300.7 pursuant to which it has agreed to be bound by Statewide Policy Guidance.

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, queriable only by Authorized Users, that provides an electronic means for identifying and locating a patient's medical records across Data Suppliers.

Registry means Research that involves use of an organized system to collect uniform data (clinical and otherwise) on a population defined by a particular disease, condition or exposure over time to evaluate specified outcomes for a predetermined scientific, clinical or policy purpose.

Research means a systematic investigation, including research development, testing and evaluation designated to develop or contribute to generalizable knowledge, including clinical trials.

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

Research Repository means the collection and storage of data with the intention for the data to be used repeatedly for research purposes, or stored for future research and/or shared with other researchers.

Researcher means an individual who is conducting Research.

Retrospective Research means Research that is not conducted in connection with Treatment and involves the use of Protected Health Information that relates to Treatment provided prior to the date on which the Research proposal is approved by the IRB.

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 technical infrastructure (SHIN-NY Enterprise) and the supportive policies and agreements that make possible the electronic exchange of clinical information among QEs,

Participants, and other individuals and entities for authorized purposes, including both the infrastructure that allows for exchange among Participants governed by the same QE and the infrastructure operated by the State Designated Entity that allows for exchange between different QEs. The goals of the SHIN-NY are to improve the quality, coordination and efficiency of patient care, reduce medical errors and carry out public health and health oversight activities, while protecting privacy and security. **Social Services Program** means a program within a social services district (as defined by New York Social Services Law, §2) which has authority under applicable law to provide "public assistance and care" (as defined by New York Social Services Law, §2), Care Management, or coordination of care and related services.

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

Statewide Collaborative Process ("SCP") means an open, transparent process to which multiple SHINNY stakeholders contribute; that is administered by the State Designated Entity for the development of Statewide Policy Guidance as provided in 10 N.Y.C.R.R. Section 300.3.

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

Statewide Policy Guidance means the set of policies and procedures, including technical standards and SHIN-NY services and products, that are developed through the Statewide Collaboration Process and adopted by NYS DOH as provided in 10 N.Y.C.R.R. Section 300.3, including the statewide policy guidance incorporated by reference in subdivision (c) of that section.

Substance Abuse and Mental Health Services Administration (SAMHSA) means a public agency within the U.S. Department of Health and Human Services (HHS). SAMHSA was established to make substance use and mental disorder information, services, and research more accessible. 42 CFR Part 2 permits patient information to be disclosed through Health Information Organizations and other health information systems.

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

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

Treatment means the provision, coordination, or management of health care and related services among health care providers or by a single health care provider, and may include providers sharing information with a third party. Consultation between health care providers regarding a

patient and the referral of a patient from one health care provider to another also are included within the definition of Treatment.

Unsecured Protected Health Information means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services in guidance issued under section 13402(h)(2) of HITECH.

Withdrawal of Consent Form means a consent form approved by Healthix under which a patient who has either given Affirmative Consent or denied consent may change his/her mind and return to a neutral consent status, only allowing access to his/her Protected Health Information in a Break the Glass situation or as otherwise provided by these Policies.

Utilization Review means an activity carried out by a Payer Organization to determine whether a health care item or service that has been provided to an enrollee of such Payer Organization, or which has been proposed to be provided to such an enrollee, is medically necessary.

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 Healthix 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 1.9.5

1.2 Exceptions to Affirmative Consent Requirement. Affirmative Consent shall not be required under the circumstances set forth in this Section 1.2. As required by Section 1.9.12, access to Protected Health Information without Affirmative Consent shall comply with applicable federal, state and local laws and regulations, including 42 C.F.R. Part 2. Protected Health Information subject to 42 C.F.R. Part 2 shall not be accessed or disclosed without Affirmative Consent unless 42 C.F.R. Part 2 specifically allows for such access or disclosure.

1.2.1 One-to-One Exchanges. Affirmative Consent shall not be required for a Transmittal of patient's Protected Health Information via Healthix originating from one Participant to another Participant if such Transmittal meets all the requirement of a One-to-One Exchange (including the requirement that the Transmittal occur with the patient's implicit or explicit consent) provided the Participants comply with existing federal and state laws

and regulations requiring patient consent for the disclosure and re-disclosure of information by health care providers.[1]

a. The Participants authorize Healthix to facilitate the One-to-One Exchange by documenting such authorization in an agreement or other form specified by Healthix.

b. If Protected Health Information is provided to a Payer Organization under a One-to-One Exchange, such exchange must comply with Section 1.9.13 which allows an individual to request restriction on the disclosure of Protected Health Information.

1.2.2 Omnibus One-to-One Exchange Agreements. Multiple Participants may enter into an omnibus One-to-One Exchange agreement that meets the requirements set forth in Subsection 1.2.1 and allows for the multiple Participants to exchange information among themselves in accordance with this Section 1.2. Upon inquiry by a Participant treating a patient (the "Querying Participant"), information from other Participants who have signed the Omnibus One-to-One Exchange Agreement will be forwarded to the Querying Participant. A list of all Participants signing an Omnibus One-to-One Exchange Agreement will be available on the Healthix website.

1.2.3 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, Healthix 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 the Healthix clinical viewer or portal without Affirmative Consent for public health purposes authorized by law, including:

i. To investigate suspected or confirmed cases of communicable disease (pursuant to PHL2(1)(1) and 10 N.Y.C.R.R. Part 2);

[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 has or had a relationship with the patient, and the information pertains to such relationship.

ii. To ascertain sources of infection (pursuant to 10 N.Y.C.R.R. Part 2);

iii. To conduct investigations to assist in reducing morbidity and mortality (pursuant to 10 N.Y.C.R.R. Part 2);

iv. As authorized by PHL 206(1)(d) to investigate the causes of disease, epidemics, the sources of mortality, and the effect of localities, employments and other conditions, upon the public health, and by PHL 206(1)(j) for scientific studies and research which have for their purpose the reduction of morbidity and mortality and the improvement of the quality of medical care through the conduction of medical audits;

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

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

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

viii. For the activities of the Electronic Clinical Laboratory Reporting System (ECLRS), the Electronic Syndromic Surveillance System (ESSS) 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. § 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 other public health purposes authorized by law and approved through the Statewide Collaboration Process and by the Healthix Board. "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. Healthix may Disclose Protected Health Information without Affirmative Consent to the New York State Office of Mental Health ("OMH") for public health purposes if Healthix Discloses Protected Health Information to NYSDOH in its role as a Public Health Agency and OMH is authorized to obtain such information under applicable state and federal law. Permissible public health purposes for disclosure to OMH shall consist of investigations aimed at reducing morbidity and mortality, monitoring of disease trends, and responding to public health emergencies, consistent with the public health activities described in Section 1.2.3(b) above.

d. A patient's denial of consent for all Participants in Healthix to access the patient's Protected Health Information through Healthix shall not prevent or otherwise restrict a Public Health Agency from accessing the patient's Protected Health Information through Healthix for the purposes set forth in Section 1.2.3(b).

e. 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, Healthix may make that disclosure on behalf of the Data Supplier or Participant without Affirmative Consent.

f. Healthix may disclose the reports and information subject to 10 NYCRR §63.4 (HIV clinical laboratory test results), for purposes of linkage to and retention in care, to Participants engaged in Care Management that have a clinical, diagnostic, or public health interest in the patient, to the extent permitted under 10 NYCRR §63.4(c)(3). Participants engaged in Care Management with a clinical, diagnostic, or public health interest in a patient may include, but are not limited to, Provider Organizations or Practitioners with a Treatment relationship with a patient, Health Homes,

and Payer Organizations providing Care Management to their enrollees. Such disclosure shall not require patient consent under applicable state and federal laws and regulations. Healthix shall work in consultation with the New York State Department of Health, AIDS Institute, prior to implementing any program under this provision.

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

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 Emergency Medical Technician to access Protected Health Information via Healthix and these individuals may Break the Glass if the following conditions are met:

   i. Treatment may be provided to the patient without informed consent because, in the Practitioner's or Emergency Medical Technician's judgment, an emergency condition exists and the patient is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the patient's life or health.

   ii. The Practitioner or Emergency Medical Technician determines, in his or her reasonable judgment, that information that may be held by or accessible via Healthix 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 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. This provision will not take effect until the necessary functionality has been deployed in the new Healthix system or when QE certification commences, whichever is sooner. Certified Applications must comply with this provision, if applicable.

   v. The Practitioner, Emergency Medical Technician or Authorized User acting under the direction of a Practitioner attests that all of the foregoing conditions have been satisfied, and the Healthix software maintains a record of this access. This provision will not take effect until the necessary functionality has been deployed in the new Healthix system or when QE certification commences, whichever is sooner. Certified Applications must also comply with this provision, if applicable.

b. Break the Glass 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. Healthix shall ensure, or shall require their Participants to ensure, that access to information via Healthix without Affirmative Consent when treating a patient pursuant to this Section 1.2.3 terminates upon the completion of the emergency treatment.

d. Notwithstanding anything to the contrary set forth in these policies, Healthix and its Participants shall not be required to exclude any Sensitive Health Information from access via Healthix where the circumstances set forth in this Section 1.2.3 are met.

e. Healthix shall promptly notify its Data Suppliers that are federally-assisted alcohol or drug abuse programs when Protected Health Information from the Data Supplier's records is accessed through Healthix under this Section. 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. This provision will not take effect until the necessary functionality has been deployed in the new Healthix system or when QE certification commences, whichever is sooner. Certified Applications must also comply with this provision.

f. Upon a patient's discharge from a Participant's emergency room, if a Break the Glass incident 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 these Policies and Procedures. In lieu of providing such notice, Participants that are hospitals may notify all patients discharged from an emergency room that their 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 by the Participant within ten days of the patient's discharge.

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 Healthix, provided that (i) Healthix is serving as the Data Supplier's Business Associate (as defined in 45 C.F.R. § 160.103) and (ii) Healthix 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 Improvement and Evaluation of Operations. Affirmative Consent shall not be required for Healthix, government agencies or their contractors to access Protected Health Information via Healthix for the purpose of evaluating and improving operations.

Consistent with HIPAA, access to PHI should be limited to the minimum amount necessary to accomplish the intended purpose of the use or disclosure. Any uses of Protected Health Information for evaluating and improving operations shall be subject to prior consideration by a subcommittee (Data Use Subcommittee) including members of the Healthix Privacy and Security Committee, the Healthix Clinical Committee, and Healthix staff. The Data Use Subcommittee will make recommendations to the Healthix Board of Directors and such uses will be subject to Board approval.

1.2.7 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 and meeting the requirements set forth in section 1.8.

1.2.8 Organ Procurement Organization Access. Healthix will provide Organ Procurement Organizations 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 Healthix to access the patient's Protected Health Information under Section 1.7.6 shall not prevent or otherwise restrict an Organ Procurement Organization from accessing the patient's Protected Health Information through Healthix for the purposes set forth in this Section 1.2.7.

1.2.9 Healthix Access for Operations and Other Purposes

Affirmative Consent shall not be required for Healthix or its contractors to access Protected Health Information to enable Healthix to perform system maintenance, testing and troubleshooting and to provide similar operational or technical support.

1.2.10 Limited Patient Care Alerts

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

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

c. Healthix shall send Limited Patient Care Alerts 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.

1.2.11 Disclosures to NYS DOH Regarding Medicaid Beneficiaries. Affirmative consent shall not be required for Healthix to Disclose Protected Health Information of Medicaid beneficiaries to NYS DOH or a Business Associate subcontractor of NYS DOH to the extent such disclosure is necessary to (i) calculate performance under quality measures adopted by the New York State Medicaid program; or (ii) determine payments to be made under the New York State Medicaid program.

1.2.12 Disclosures to Payer Organizations for quality measures. Affirmative Consent shall not be required for HEALTHIX to Disclose Protected Health Information to a Payer Organization (including NYS DOH in regards to its operation of the New York State Medicaid program) or a Business Associate of a Payer Organization to the extent such Disclosure is necessary to (i) calculate performance of HEDIS or QARR measures; or (ii) in the case of disclosures to NYS DOH, determine payments to be made under the New York State Medicaid program.

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

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

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

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

c. Protected Health Information originating from a facility subject to the New York Mental Hygiene Law is Disclosed only if the facility has

requested that an investigation be conducted into the death of a patient and the recipient is a Medical Examiner or Coroner that is licensed as physician or nurse practitioner.

1.2.15 Telehealth

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

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

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

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

iv. The Participant does not Access or receive any Protected Health Information subject to 42 C.F.R. Part 2 or New York Mental Hygiene Law § 33.13 unless the patient has provided consent in written or electronic form and a signature that is recognized by the Electronic Signatures and Records Act (NY State Tech Law §301 *et seq*), including an oral signature recording to the extent recognized under that act; and

v. The Participant Accesses or receives the patient's Protected Health Information only during the time period specified in subsection 1.2.13(b).

b. The patient's verbal consent for Telehealth services shall remain valid for the duration of the telehealth visit. A new verbal consent, in accordance with Section 1.2.15 (a) will need to be obtained for each visit.

1.2.16 Health Oversight Agencies.

a. A Health Oversight Agency may access Protected Health Information through the Healthix clinical viewer or portal without Affirmative Consent for health oversight purposes authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

b. a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

i. The receipt of health care;

ii. A claim for public benefits related to health; or

iii. Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

1.3 Form of Patient Consent. Except as otherwise permitted by the Patient Consent Transition Rules set forth at Section 1.10, consents shall be obtained through an Approved Consent. Healthix may approve an alternative to a Level 1 Consent or Level 2 Consent if the Alternative Consent includes the information specified in this section. As required by Section 1.9.12, Healthix is responsible for ensuring that any approved Alternative Consents comply with applicable federal, state and local laws and regulations. If an Alternative Consent is to be used as a basis for exchanging information subject to 42 C.F.R. Part 2, Healthix shall ensure that such form meets the requirements of 42 C.F.R. Part 2. Use of a Health Home Consent form is authorized after review and approval by Healthix.

1.3.1 Level 1 Uses. Affirmative Consent to access information via Healthix for Level 1 Uses shall be obtained using a Level 1 Consent or an Alternative Consent approved by Healthix under this Section 1.3.1, which shall include the following information:

a. A description of 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, if such categories of information may be disclosed to the recipient;

b. The intended uses to which the information will be put by the Participant. A general description, such as "for treatment, care management or quality improvement" shall meet this requirement;

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

d. Signature of the patient or the patient's Personal Representative. If the consent language required under subsections 1.3.1. (a), (b) and (c) above is incorporated into another document such as a health insurance enrollment form in accordance with Section 1.3.4.(c), the signature need not appear on the same page as the language required under subsections 1.3.1. (a), (b) and (c) above.

1.3.2 Level 2 Uses. Consent to access information via Healthix for the purposes of Level 2 Uses shall be obtained using a Level 2 Consent or an Alternative Consent approved by Healthix under this Section 1.3.3, which shall include (i) the information required pursuant to Section 1.3.1 and (ii) the following information:

a. The specific purpose for which information is being accessed, which, with respect to Research, including a Research database or repository, may be expressed broadly to include future Research purposes, provided that such expression is permitted under the Statewide Policy Guidance;

b. Whether Healthix 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

e. A list 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 patient to access an up-to-date list of Data Suppliers through the Healthix website or other means; the consent form shall also identify whether Healthix 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 form the Healthix website or by other means;

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

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

h. The date of execution of the consent.

1.3.3 Requirement for Separate Consents.

a. Consent for Level 1 Uses and consent for Level 2 Uses shall not be combined.

b. Consent for different Level 2 Uses shall not be combined.

c. A consent for a Level 1 or Level 2 Use shall not be combined with any other document except with the approval of Healthix. If Healthix agrees to allow an Alternative Consent that is combined with a health insurance enrollment form, such Alternative Consent shall expire no later than the date on which the patient's health insurance enrollment terminates.

1.3.4 Education Requirement for Level 2 Consents Relating to Marketing. When a Healthix or its Participant obtains a Level 2 Consent to access Protected Health Information via Healthix for the purpose of Marketing, Healthix or its Participant must provide the patient with information about the nature of such Marketing. Notwithstanding the foregoing, Healthix does not currently allow use of Protected Health Information for Marketing purposes.

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 [LEFT INTENTIONALLY BLANK]

1.4.3 Redisclosure Warning

a. Healthix, and/or Certified Applications, 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. Healthix shall coordinate with Participants using Certified Applications in order to allow them to satisfy this requirement.

b. Healthix and/or Certified Applications 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. Healthix will satisfy this requirement by placing such a redisclosure warning on the log-in screen that Authorized Users must view before logging into their EHR or otherwise accessing Healthix.

c. Healthix and/or Certified Applications 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 redisclosed except as permitted by the New York Mental Hygiene Law. Healthix will satisfy this requirement by placing such a redisclosure warning on the log-in screen that Authorized Users must view before logging into their EHR or otherwise accessing Healthix. This provision will take effect when the necessary functionality is deployed in the new Healthix system or when QE certification commences, whichever is sooner. Certified Applications must also comply with this provision.

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 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 General:

a. Healthix and its Participants will permit the exchange of information about Minors based on an Affirmative Consent executed by the Minor's Personal Representative, provided that Healthix will not disclose such information received from facilities regulated by SAMHSA under 42 CFR Part 2.

b. Notwithstanding section 1.5.2a, Healthix and its Participants may not disclose Minor Consent Information obtained through Healthix to the minor's Personal Representative without the Minor's written consent. Healthix shall provide or arrange for training for its Participants on compliance with this section 1.5.2.b, and shall include a notice warning against such re-disclosure on any display of a Minor's information on the Healthix portal and in any record of a Minor's information that Healthix provides.

c. Participants who perform services that generate Minor Consent Information may designate to Healthix its Authorized Users who perform such services (such User to be referred to as a "Provider of Minor Consented Services").

d. Notwithstanding any consent decision made by a Minor's Personal Representative, a Minor may give consent in a form acceptable to Healthix, to designate and authorize a Provider of Minor Consented Services to access all of the Minor's information in Healthix during the current encounter, which shall be the duration of the ambulatory visit or inpatient admission in which the Minor gives such consent (such consent

to be referred to as a "One Time Override"). Upon assertion by the Provider of Minor Consented Services that a Minor has given such consent, Healthix shall disclose such information to the Provider of Minor Consented Services. Healthix shall audit, or shall require the Participant to audit, each such assertion.

1.5.2 Implementation. Section 1.5.1 will take effect when the necessary functionality is deployed in the new Healthix system or when QE certification commences, whichever is sooner. Certified Applications must also comply with this provision.

1.5.3 Transition from Minor Status. Neither Healthix nor its Participants shall exchange Protected Health Information about patients age 18 years or older based on an Affirmative Consent of the patient's parent or legal guardian provided while the patient was a minor unless the parent or legal guardian continues to be the patient's Personal Representative.

1.6 De-Identified Data and Limited Data Sets.

1.6.1 Access of De-Identified Data and Limited Data Sets for Specified Uses. Affirmative Consent shall not be required for the following purposes:

a. Access to De-Identified Data or a Limited Data Set via Healthix by a Participant or government agency that is approved in accordance with Section 1.8, for:

i. Research reviewed and approved or granted a waiver by an Institutional Review Board (IRB) organized and operating in accordance with 45 C.F.R. § 164 and Section 1.8 below, and provided that (a) Healthix shall enter into a data use agreement with the Researcher prior to disclosing a Limited Data Set in accordance with the HIPAA Privacy Rule, and (b) the Data Supplier(s) that are the source of the Protected Health Information in a Limited Data Set have not withdrawn their consent to allow for disclosures of their Protected Health Information in the form of a Limited Data Set for purposes of Research; or

ii. Any purpose for which Healthix, Participant, or government agency may lawfully access Protected Health Information under the Policies and Procedures.

b. Access to De-Identified Data or a Limited Data Set via Healthix by an entity that is not eligible under Healthix Policy to be a Participant, for Research reviewed and approved or granted a waiver by an Institutional Review Board organized and operated in accordance with 45 C.F.R. §164, provided that:

i. Such entity is a not-for-profit organization whose mission is consistent with the mission of Healthix and its Participants, and

ii. Such entity and research is approved by the Research Committee as specified in Section 1.8 below, and

iii. Such entity is approved by the Board of Directors to conduct Research using data via Healthix, and

iv. Healthix shall enter into a data use agreement with the Researcher prior to disclosing a Limited Data Set in accordance with the HIPAA Privacy Rule, and

v. The Data Supplier(s) that are the source of the Protected Health Information in a Limited Data Set have not withdrawn their consent to allow for disclosures of their Protected Health Information for purposes of Research.

c. Access by Healthix to De-Identified Data or Limited Data Sets to advise a third party that is designing a clinical trial or study, as to the feasibility of identifying sufficient potential subjects to meet the qualifying criteria being considered for the clinical trial or study, provided that (i) the Research Committee described in Section 1.8.(a)(i) has granted approval for Healthix to perform this service for the clinical trial or study and (ii) the Data Supplier(s) that are the source of the Protected Health Information in a Limited Data Set have not withdrawn their consent to allow for disclosures of their Protected Health Information for purposes of Research.

d. Disclosure of De-Identified Data by Healthix so long as (i) the disclosure is in keeping with the mission of the SHIN-NY, (ii) Healthix enters into a data use agreement with the recipient that contains the provisions set forth in Section 1.6.1(e); and (iii) the disclosure is consistent with Healthix Business Associate Agreement and Participation Agreement with the applicable Participant(s).

e. The data use agreement required under Section 1.6.1(d) must:

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

ii. Prohibit the recipient from re-identifying or attempting to re-identify the De-Identified Data.

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

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

v. Mandate that the recipient may not disclose the De-Identified data to any third party unless the agreement explicitly permits such a Disclosure and the third party also agrees in writing to follow the restrictions set forth in this Section 1.6.

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

1.6.3 Other Requirements.

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

b. Healthix shall not condition a patient's participation in Healthix on the patient's decision to consent or deny access to De-Identified Data or Limited Data Sets for purposes other than those set forth in Section 1.6.1.

c. Healthix shall and shall require Participants to comply with standards for the de- identification of data set forth in 45 C.F.R. § 164.514 when using information from Healthix.

d. Healthix 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 Use of Protected Health Information for Research. Protected Health Information obtained via Healthix may be used for Research provided that (a) the Research is approved as described in Section 1.8 and has IRB approval as described in Section 1.8.3(a)(xii), and (b) the Researcher obtains the Level 2 Consent described in Section 1.3.2.

1.7.1 Use of Protected Health Information for Retrospective Research. Affirmative Consent shall not be required for Healthix to disclosed Protected Health Information to a Researcher conducting Retrospective Research if: (i) an IRB and/or a Privacy Board has approved of such disclosure, and (ii) the Research Committee has approved of such disclosure, and (iii) the Data Supplier(s) that are the source of the Protected Health Information have agreed to allow for disclosures of their Protected Health Information for purposes of Research.

1.7.2 Use of Protected Health Information for Patient Recruitment for Research. Affirmative Consent shall not be required for Healthix to review Protected Health Information on behalf of a Researcher to determine which individuals may qualify for a Research study. In addition, Affirmative Consent shall not be required for Healthix to

disclose the name and other identifying information of an individual who may qualify for a Research study to a Participant that has a treating relationship with such individual so that the Participant may contact the individual to determine his or her willingness to participate in such study, provided that all of the following requirements are met:

a. An IRB has approved of such disclosure;

b. The Research Committee has approved of such disclosure;

c. The Data Supplier(s) that are the source of the Protected Health Information have agreed to allow for the disclosure of their Protected Health Information for purposes of Research; and

d. The disclosure does not include any mental health clinical information governed by Section 33.13 of the Mental Hygiene Law, unless the Participant receiving the disclosure is a facility as defined in the Mental Hygiene Law.

1.7.3 Participant Consent for Research. Solely with respect to Sections 1.7.1(iii) and 1.7.2(c), and with respect to access to Limited Data Sets in Section 1.6.1, each Participant that supplies Protected Health Information to Healthix as a Data Supplier, as a condition of participation, automatically consents to the disclosure of its Protected Health Information for purposes of Research as required under Sections 1.7.1(iii) and 1.7.2(c) and with respect to Limited Data Sets in Section 1.6.1, unless such Participant informs Healthix in writing and in a form acceptable to Healthix that it wishes to withdraw such consent. In the event that the Participant withdraws such consent, it shall retain the ability, in its sole discretion, to grant consent, in writing and in a form acceptable to Healthix, for the disclosure of its Protected Health Information for the limited purposes of a specific Research study.

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

a. The researcher shall present the proposed research to Healthix for initial screening. If the QE determines the proposed Research project is appropriate, the proposal shall be submitted to the Centralized Research Committee for approval, in lieu of approval by a Healthix Research Committee, if:

i. the researcher would receive Protected Health Information that does not solely consist of a Limited Data Set, or

ii. the researcher would receive De-Identified Data or a Limited Data Set and the policies adopted by one of the QEs that is the source of such information would require approval by the QE Research Committee of such QE. Notwithstanding the foregoing, if the researcher would obtain information from only two (2) QEs, then approval by the Centralized Research Committee is not necessary if

the QE Research Committee of one such QE approves the Research and the other QE consents to such approval.

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

c. If Healthix receives information from another QE for a Research project it shall keep such information separate from other information maintained by Healthix. Healthix ensure that such information is only used for the Research project for which it was obtained and shall delete such information from its systems within a reasonable time period after the Research is completed. Healthix shall have no obligation to correct errors in the information it receives from another QE.

1.8 Additional Research Requirements.

1.8.1 Research Committee. The Healthix Board shall designate a Research Committee to approve applications under this Section.

a. The Research Committee shall be organized to review and approve Research proposals. The committee shall (1) have members with varying backgrounds and appropriate professional competency as necessary to review the effect of the Research protocol on individuals' privacy rights and related interests; (2) include at least one member who is not an employee, contractor, officer or director of Healthix or any entity conducting the research, and is not related to any person who meets any of the foregoing criteria; and (3) not have any member participating in a review of any project in which the member has a conflict of interest.

1.8.2 Conditions. Subject to the provisions of Sections 1.6 and 1.7, Protected Health Information or De-identified Data or Limited Data Sets (for purposes of this Section 1.8, referred to collectively as "Data") from Healthix can be accessed, used or disclosed for Research purposes provided the following conditions are met:

a. The Researcher must be employed by a Healthix Participant, or by a non-Participant that meets the requirements in Section 1.6.1.b.i, ii and iii.

b. The Researcher and the entity that employs the Researcher must be approved by the Research Committee.

c. The specific use as permitted in this Section must approved by the Research Committee.

d. The Research Committee shall review applications as described in Section 1.8.3 to determine that the proposal meets the following criteria for approval:

i. Compliance with Research policy: Healthix staff shall confirm that the proposal is consistent with Healthix Policy, before forwarding the proposal to the Research Committee

ii. Feasibility of Healthix support: Healthix staff shall confirm that Healthix contains the data required by the proposal, and shall determine the feasibility and resource requirements of extracting such data, before forwarding the proposal to the Research Committee

iii. Meeting the definition of Research: The Research Committee shall confirm that the proposed study meets the definition of Research rather than generating market intelligence, competitive advantage, commercial promotion, or other purposes that are not Research

iv. Not compromising the reputation of Healthix or its Participants: the Research Committee shall determine that the study is not intended to reduce the good reputation of Healthix or any of its Participants

v. Respecting the privacy of Participant and Patient data: The applicant shall commit to adhere to Healthix Policy, including Section 1.8.6

vi. Research that involves creation of a Registry or Research Repository must obtain additional approvals under Section 1.8.2.e below

vii. Other requirements of Healthix: The entity that employs the Researcher, and the application itself, shall be reviewed by the Research Committee to establish overall compliance with the mission and purpose of Healthix and its Participants as well as compliance with such other criteria as the Research Committee deems appropriate for the Research in question and the protection of Healthix. On behalf of Healthix, the Research Committee retains discretion in its determination as to whether to approve or reject any and all Research.

e. In the event that Data provided by Healthix will be incorporated into a Registry or Research Repository, approval by the Research Committee shall be required after its consideration of the following additional concerns:

i. The purpose of the Registry or Research Repository,

ii. The limits on future uses of the Data in the Registry or Research Repository;

iii. Designation of Researchers who may have access to the Data in the Registry or Research Repository in the future;

iv. Whether additional authorizations by Healthix will be required prior to access to the Data in the Registry or Research Repository for future uses or by future Researchers;

v. In the event that Healthix provides Protected Health Information to the Registry or Research Repository, whether additional Consent by the patient will be required prior to future uses of the Data;

vi. The time period during which the Data will remain in the Registry or Research Repository. In the event that the Research Committee approves the proposal, the approval will specify an end date of no more than five (5) years after the approval date, beyond which the Data may remain in the Registry or Research Repository only if the Research Committee subsequently approves a continuation application submitted by the Researcher extending to it to a new specified future date not to exceed five years from the date of the continuation application.

In the event that the Research Committee requests a consultation with the Privacy Committee regarding such concerns, the Privacy Committee shall designate a subgroup for such consultation.

f. To fulfill its obligations under this Section 1.8 the Research Committee shall develop and apply procedures that specify at a minimum:

i. Which decisions of the Research Committee require a synchronous meeting, whether in-person, electronic or telephonic, and which can be made by asynchronous communication such as an email exchange, among its members

ii. The quorum required for specific types of decisions

iii. The majority threshold required for specific types of decisions

iv. A process for individual members to appeal a decision before implementation.

1.8.3 **<u>Application</u>**. In order to request Healthix approval for access, use or disclosure of Data for a Research purpose, an application must be submitted to the Research Committee.

a. Such application must be limited to two pages in a format approved by Healthix and must include, at a minimum:

i. Objectives;

ii. Methods;

iii. A detailed list of data elements requested;

iv. Study period (i.e., the time period during which the study will be conducted or the Registry or Research Repository will be maintained);

v. Data collection period (i.e., the time period during which the data was entered into Healthix (the origination dates of the data));

vi. A list of Healthix Participants whose Data will be excluded from the proposed Research or a statement that Data of all Participants will be included;

vii. Study population (i.e., inclusion and exclusion criteria for patient cohort definition, or a statement that data of all Healthix patients may be included);

viii. External funding (i.e., any funding in support of the proposed Research not provided by the entity that employs the Researcher);

ix. Dissemination plan (i.e., the intended use of the results of the study, including publication or public presentation, and a commitment to share the results with Healthix prior to publication, to notify Healthix of any publication or public presentation, and to credit Healthix in any such publication or public presentation);

x. Investigation team (i.e., a list of all members of the proposed investigation team with titles and affiliations);

xi. A statement of whether consultations or substantial intellectual contributions by Healthix may be required in the course of the study;

xii. Written proof of IRB approval or exemption or a written determination that the Research is not human subject research (not included in the 2-page limit);

xiii. A detailed description of the data security measures that will be implemented (not included in the 2-page limit); and

xiv. A statement that the Researcher agrees to comply with all Healthix policies.

b. In the event that the application is for Healthix to provide Data to a Registry or Research Repository, the application will further specify the information described in Section 1.8.2.e.

c. After submission of a complete application, Healthix will review the feasibility of providing the Data.

d. If deemed feasible, the application will then be presented to the Research Committee for review and final action, and such final action shall be communicated in writing to the requesting Researcher.

1.8.4 Fees.

a. If approved, Healthix will provide a work order with estimated costs to cover the data extraction and the applicant will sign the work order agreement to reimburse Healthix for such costs. Any change in scope of work may entail additional charges that would have to be mutually approved.

b. Healthix will establish a standard fee schedule to use Data for Research purposes, and the applicant will agree to pay such fees. The fee schedule shall take into account the purpose, scope and funding source of the Research and the type of Researcher. Healthix will periodically review the standard fee schedule with the Finance Committee.

1.8.5 Modifications. To the extent that IRB approval is required for: (i) modifications to the original protocol; (ii) change in the composition of the investigation team; or (iii) extensions of the approved study period, a written application must be submitted to, and approved by, Healthix or the Research Committee prior to proceeding with the revisions.

1.8.6 Prohibitions. Researchers are prohibited from:

a. combining the Healthix Data with any other source without prior approval by Healthix;

b. re-identifying any of the De-identified Data provided by Healthix;

c. presenting or disseminating information resulting from analyses done on Healthix information if a provider organization or any of its component elements (e.g., departments, clinics, affiliates, etc.) may be easily identified either by name or association, unless the Research Committee and the identifiable participant have granted prior approval for such presentation or dissemination;

d. sharing Data with any individual who is not a member of the investigation team as listed on the original application or approved modification, except to the extent that the Research involves the creation of a Registry or Research Repository, which creation otherwise meets the requirements of

these Policies and Procedures and the Statewide Policy Guidance, and only to the extent that any sharing otherwise meets all of the requirements of these Policies and Procedures, the Statewide Policy Guidance and all applicable laws, including, without limitation, all laws applicable to Research;

e. using Data for purposes other than those expressly described in the original application and approved modification.

1.8.7 Security. All Data shall be stored using standard data security methods (e.g., as applicable, encryption of electronic data, stored in locked office/file cabinet).

1.8.8 Termination of Research. All Data shall be returned to Healthix or destroyed at the end of the approved study period.

1.8.9 Periodic Updates. Healthix will periodically inform Participants of ongoing Research projects.

1.9 Other Policies and Procedures Related to Consent.

1.9.1 Affiliated Practitioners. An Affirmative Consent obtained by a Participant shall apply to an Affiliated Practitioner of the Participant provided that (a) such Affiliated Practitioner is providing health care services to the patient at the Participant's facilities; (b) 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 (c) such Affiliated Practitioner is providing health care services to the patient in the course of a cross-coverage or on-call arrangement with the Participant or one of its Affiliated Practitioners.

1.9.2 Authorized Users. An Affirmative Consent obtained by a Participant shall permit Authorized Users of the Participant to access information covered by the Affirmative Consent in accordance with Sections 2 and 4.

1.9.3 Consents Covering Multiple Participants. An Affirmative Consent may apply to more than one Participant provided that the consent lists each Participant with sufficient specificity to provide reasonable notice to the patient as to which Participants may access the patient's information through Healthix pursuant to such consent. Any Participant accessing information based on a consent covering multiple Participants must be identified on such consent at the time the patient grants Affirmative Consent.

a. Except as described in Section 1.9.3(b) below, 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 Participants listed on the Affirmative Consent confirm in writing and provide acceptable evidence to Healthix that they (i) are part of an organized health care arrangement ("OHCA") as defined by HIPAA, and (ii) share a single medical record, the patient does not need to be given the

option outlined in Section 1.9.3(a). Acceptable evidence of (ii) may include that the OHCA and its Participants maintain only a single instance of an EHR, and for each patient, only a single medical record number.

1.9.4 Consent Obtained by Healthix. Healthix may obtain consents on behalf of their Participants, provided such consents meet all of the requirements set forth in this Section 1.

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

1.9.6 Denial of Consent. A Level 1 or Level 2 Consent shall give the patient the option of granting or affirmatively denying consent for individual Participants to access information about the patient via Healthix. A patient's decision not to sign a consent shall not be construed as a "denial of consent" under Section 1.2.3(a)(iii). Healthix hall ensure that patients have the option, through the use of a single paper or electronic form, to affirmatively deny consent for all Participants in Healthix to access the patient's information, except as set forth in Section 1.2.2(b) or Section 1.2.7. This provision will become effective when the necessary functionality is deployed in the new Healthix system or when QE certification commences, whichever is sooner. Certified Applications must also comply with this provision.

1.9.7 Durability. An Affirmative Consent for Level 1 Uses does not have to be time-limited. An Affirmative Consent for Level 2 Uses shall be time-limited and shall expire no more than two years after the date such Level 2 Consent is executed, except to the extent a longer duration is required to complete a Research protocol. If the Level 2 Consent is used for Research, including a Registry or Research Repository, it is not necessary for the Level 2 Consent to be time limited and a statement on expiration such as "end of the Research study,", "none," or other similar language is sufficient, provided that such statement is permitted under the Statewide Policy Guidance.

1.9.8 Revocability. Patients shall be entitled to revoke an Affirmative Consent at any time provided that such revocation shall not preclude any Participant that has accessed Protected Health Information via Healthix prior to such revocation and incorporated such Protected Health Information into its records from retaining such information in its records. When revoking consent, patients may complete a Withdrawal of Consent Form that will reflect their wish to return their consent status to neutral.

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

1.9.10 Compliance with Business Associate Agreements with Data Suppliers. Healthix shall execute a Business Associate Agreement with each Data Supplier. Healthix shall not use or disclose Protected Health Information in any manner that violates the Healthix Business Associate Agreements.

1.9.11 Disclosure to Healthix Vendors. Healthix, acting under the authority of a Business Associate Agreement with its Participants, may disclose Protected Health Information to vendors that assist in carrying out Healthix authorized activities provided (i) Healthix requires the vendors to protect the confidentiality of the Protected Health Information in accordance with Healthix Business Associate Agreements with its Participants and (ii) the vendor does not make such information available to a Participant that has not obtained Affirmative Consent.

1.9.12 Compliance with Existing Law. All access to Protected Health Information via Healthix 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.

1.9.13 Compliance with Requests for Restrictions on Disclosures to a Payer Organization. Healthix shall develop processes to ensure that a Payer Organization does not access Protected Health Information through Healthix 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. Healthix 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 Healthix 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.

c. All Healthix Participants shall either: (i) Notify Healthix immediately upon receipt of any such patient's request that PHI not be disclosed to a Payer Organization; or (ii) Refrain from sending PHI related to any encounter for which a patient has requested his/her PHI not be disclosed to a Payer.

1.9.14 Development of Policies Governing Disclosures to Government Agencies for Health Oversight. Healthix will only respond 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, if required by laws. Healthix will not disclose such information in instances where disclosure is permitted but not required by law. Healthix will notify its Participants of all such requests. This section does not cover access to Protected Health Information by Public Health Agencies under Section 1.2.2.

1.9.15 Indication of Presence of Medical Order for Life Sustaining Treatment ("MOLST") or Other Advance Directive. Healthix may note whether a patient has signed a MOLST or other advance directive in a Record Locator Service or Other Comparable Directory without Affirmative Consent.

1.9.16 Consent for Access by ACOs and IPAs. An Affirmative Consent authorizing access by an ACO or IPA shall cover only the ACO or IPA entity itself and not the health care providers participating in the ACO or IPA.

1.9.17 Subpoenas. Healthix will inform Participants of any subpoena for access to their Protected Health Information, unless otherwise prohibited by law, in sufficient time to allow Participant to raise any legal defenses regarding such disclosure. Healthix will only respond to subpoenas if required by law and shall, upon request, cooperate with Participant in raising legal defenses regarding disclosure of Protected Health Information.

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

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

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

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

d. Healthix reasonably believes that the disclosure is in accordance with state and federal law and the terms of the Business Associate Agreement.

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

f. The Business Associate agrees not to further disclose the Protected Health Information except where these Policies and Procedures allow for such disclosure.

1.10 Patient Consent Transition Rules.

1.10.1 Use of Approved Consents. Except as set forth in Section 1.8.2, Healthix shall be required to utilize an Approved Consent (and/or a modified Approved Consent form, provided such modifications have been approved by DOH) or Health Home Consent with respect to all patients who consent to the exchange of Protected Health Information via Healthix *on or after* the Consent Implementation Date.

1.10.2 Reliance on Existing Consents Executed Prior to the Consent Implementation Date. Patient consents that were substantially similar to a Level 1 Consent *prior to* the Consent Implementation Date (an "Existing Consent Form") may continue to be relied 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 NYS DOH.

1.11 Receipt of Patient Care Alerts.

1.11.1 A Participant may receive Patient Care Alerts from Healthix with respect to any patient from whom the Participant has obtained Affirmative Consent.

1.11.2 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.

1.12 Access for Disaster Tracking.

1.12.1 For the purpose of locating patients during an Emergency Event, a Disaster Relief Agency shall be allowed to access the following information through Healthix without Affirmative Consent:

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

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

1.12.2 Access to information under this section may begin when the Emergency Event begins and shall cease when the Emergency Event ceases.

1.12.3 If a Disaster Relief Agency accesses information under this section during an Emergency Event for the purpose of locating missing persons, the Disaster Relief Agency may continue to utilize such information after the Emergency Event ceases, while the missing persons investigation is open, provided that such utilization shall be limited to the purpose of locating persons reported as missing during the Emergency Event.

1.12.4 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.

1.12.5 A patient's denial of consent for all Participants in Healthix to access the patient's Protected Health Information under Section 1.7.6 shall not restrict a Disaster Relief Agency from accessing information as permitted by this section.

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

1.13.1 The patient has granted Affirmative Consent for the Transmittal, provided that Affirmative Consent shall not be required if the Transmittal is provided to a public health authority, as defined at 45 CFR § 164.501. The Affirmative consent shall meet all the requirements of a Level 1 Consent or Alternative Consent, provided that if the recipient is a life or disability insurer that is not a government entity then the form shall have been approved by the applicable department(s) of insurance. For the avoidance of doubt, none of the exceptions to the Affirmative Consent requirement set forth in Section 1.2 other than section 1.2.2 shall apply to Transmittals under this section.

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

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

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

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

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

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

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

1.13.5 Healthix enters into an agreement with the recipient that requires the recipient to:

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

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

c. Notify Healthix in writing and in the most expedient time possible if the recipient becomes aware of any actual or suspected Breach of Unsecured Protected Health Information; and

d. Represent that the recipient is not excluded, debarred, or otherwise ineligible form participating in any federal health care programs.

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

1.13.6 Nothing in this Section 1.13 shall be construed to prohibit a patient from disclosing any of the patient's Protected Health Information the patient has received from Healthix under Section 5.2 to an individual or entity of the patient's choice.

1.14 Waivers During a Public Health Emergency. NYSDOH may waive provisions in this Section 1 and other provisions of these Policies and Procedures during a public health emergency under Section 319 of the Public Health Services Act if

1.14.1 the waiver assists QEs and/or their Participants in their response to the public health emergency;

1.14.2 NYSDOH provides public notice of such waiver; and

1.14.3 The waiver complies with applicable state and federal law.

SECTION 2: AUTHORIZATION

Purpose/Principles

Authorization is the process of determining whether a particular individual within a Participant has the right to access Protected Health Information via Healthix. 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 Healthix and their Participants shall follow when establishing role-based access standards and authorizing individuals to access information about a patient via Healthix. 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 Healthix.

Policies and Procedures

2.1 Role-Based Access Standards.

2.1.1 Attachment A is a matrix of the categories of Authorized Users established by Healthix, including:

a. the name of each category of Authorized Users;

b. the purposes for which Authorized Users in those categories may access Protected Health Information via Healthix;

c. the types of Protected Health Information that Authorized Users within such categories may access (e.g., demographic data only, clinical data).

2.1.2 In establishing categories including the purposes for which Protected Health Information can be accessed and the types of Protected Health Information that can be accessed, Healthix will consider the Authorized User's job function and relationship to the patient.

2.1.3 At a minimum, Healthix 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. 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. Provider of Minor Consented Services;

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

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

f. Healthix administrators with access to non-clinical information;

g. Healthix 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

h. Healthix 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.

This provision will take effect when the necessary functionality is deployed in the new Healthix system or when QE certification commences, whichever is sooner. Certified Applications must also comply with this provision.

2.1.4 Participants shall designate the individuals within their organizations who will be authorized to access information via Healthix and to assign those individuals to the appropriate categories as listed above. Participants may designate such users and roles via LDAP and/or Active Directory to Healthix.

2.1.5 Healthix 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 Healthix or Participant may deem appropriate given their security risk assessment.

2.1.6 Healthix permits Certified Applications to access Protected Health Information via Healthix in accordance with the terms of these Policies and Procedures. Healthix will ensure that the certification process for Certified Applications satisfies all encryption and other security standards incorporated into the Statewide Policy Guidance 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 Healthix is who he or she claims to be. This is accomplished by providing proof of identity. This Section 3 sets forth minimum requirements that Healthix and its Participants shall follow when authenticating individuals prior to allowing them to access information via Healthix. 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. Healthix 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 Healthix. Such authentication shall take place in accordance with the provisions of this Section 3. Currently, Healthix delegates all initial identity-proofing to its Participants.

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

3.3 Option to Rely on Statewide Authentication Service. In the event that New York State develops statewide services for the authentication of Authorized Users, Healthix may utilize such statewide services to authenticate an Authorized User in accordance with the provisions of this Section 3.

3.4 Authentication of Certified Applications and Downstream Users. In regard to Certified Applications, Healthix must (i) implement systems consistent with the Statewide Policy Guidance 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 Procedures outlined in the Appendix B.

SECTION 4: ACCESS

Purpose/Principles

Access controls govern when and how a patient's information may be accessed by Authorized Users through Participants. This Section 4 sets forth minimum behavioral controls Healthix shall implement to ensure that: 1.) only Authorized Users and Certified Applications access information via Healthix; 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.** Healthix shall, or shall require its 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 Healthix. In doing so, Healthix and/or its 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 800-63-2 (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 in accordance with the NIST SP 800-63 guidelines, as may be revised from time to time.

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.

4.1.6 Passwords shall not exist in batch jobs, scripts or terminal function keys, and shall never be stored in readable form in files or databases.

4.1.7 Passwords may not under any circumstances by conveyed using any electronic method (including email) unless adequate security measures have been put into place to ensure that the passwords will not be intercepted or otherwise accessed by anyone other than the person to whom such information is intended to be conveyed.

4.2 **Authorized Purposes.** Healthix and its Participants shall permit Authorized Users to access Protected Health Information via Healthix only for purposes consistent with a patient's Affirmative Consent or an exception set forth in Section 1.2

4.3 **Failed Access Attempts.** Healthix shall enforce a limit of consecutive Failed Access Attempts by an Authorized User. Upon a fifth Failed Access Attempt, Healthix shall

ensure that said Authorized User's access to Healthix is disabled either by locking the account until release by a Healthix administrator or by locking the account for a specific period of time as specified by Healthix, after which the Authorized User may reestablish access using appropriate identification and authentication procedures. If Authorized Users access Healthix by logging on to a Participant's information system (without the need for a separate Healthix log-on), Healthix may delegate to the Participant responsibility for enforcing this Failed Access Attempt limitation.

4.4 **Periods of Inactivity.** Healthix shall ensure that an Authorized User is automatically logged out of Healthix after a period of system inactivity of fifteen (15) minutes by such Authorized User or, in the case of (i) Authorized Users who access Healthix via Participant's own system; or (ii) Participants using Certified Applications, such other period of time as Healthix determines is reasonable in light of risk analysis and organizational factors of Participant such as current technical infrastructure, hardware and software security capabilities. In addition, Authorized User's access must be inactivated after a period of inactivity of 180 days by such Authorized User. The termination shall remain in effect until the Authorized User reestablishes access using appropriate identification and authentication procedures.

4.5 **Access Limited to Minimum Necessary Information.** Healthix shall, and shall require its Participants to, ensure that reasonable efforts are made, except in the case of access for Treatment, to limit the information accessed via Healthix 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, Healthix 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.** Healthix shall implement, either directly or through Participants, minimum training requirements for educating individuals about the policies and procedures for accessing Protected Health Information via Healthix as specified by the Statewide Collaboration Process

4.7.1 Healthix shall, or shall require its Participants to, provide either on-site training, web-based training, or comparable training tools so that Authorized Users are familiar with the operation of Healthix and these Policies and Procedures.

4.7.2 Healthix shall, or shall require their Participants to, ensure that each Authorized User undergoes such training prior to being granted access to information via Healthix.

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

4.7.4 Healthix shall 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 Healthix. Healthix 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. Healthix shall establish procedures to be followed when a Participant's, Authorized User's or Data Supplier's access to, or connection with, Healthix is terminated.

4.8.1 Healthix shall ensure that access to Healthix by a Participant (and all of the Participant's Authorized Users, if applicable) or Authorized User, as 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 Healthix;

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; and/or

c. As otherwise required in these Policies and Procedures.

4.8.2 Healthix requires its Participants to notify Healthix 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 Healthix shall establish sanctions to redress policy or procedural violations. Sanctions could include temporary access prohibitions, re-training requirements, termination, or other processes Healthix deems necessary in accordance with its internal risk analyses.

4.9 Access by Certified Applications.

4.9.1 Notwithstanding anything to the contrary in this Section 4, Healthix 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, Participant using a Certified Application are required to provide Healthix 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 is required 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 Participants using a Certified Application are required 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 Healthix. Participants are required to credential, train and otherwise manage the access of such users to Protected Health Information obtained through Healthix 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, Healthix 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 Healthix 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 Healthix that obligates the Practitioner(s) to abide by the relevant terms of the Provider Organization's Participation Agreement with Healthix and engage in bi-directional exchange of Protected Health Information through the SHIN-NY.

b. The Provider Organization, under its Participation Agreement with Healthix, 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 Healthix, accepts liability for the acts and omissions of such Practitioners for violations of the Provider Organization's Participation Agreement with Healthix 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 Healthix through the Provider Organization under Section 4.10.2, each Practitioner or medical group entering into a written agreement with the Provider Organization shall be treated as a separate Participant for purposes of implementing the patient consent requirements of these Policies and Procedures.

4.10.4 Sections 4.10.2 and 4.10.3 shall not apply to Practitioners when they are acting as Affiliated Practitioners of a Provider Organization under Section 1.9.1.

4.11 Agents

4.11.1 A Participant may authorize an Agent to receive Protected Health Information from Healthix on behalf of the Participant. The Agent may only receive Protected Health Information that the Participant is permitted to receive pursuant to this Policy and the Statewide Policy Guidance.

4.11.2 In order to disclose information to an Agent, Healthix must receive written instructions and authorization from the Participant indicating that the Agent is acting on behalf of the Participant. Such authorization must specifically state that the Participant will inform Healthix if the Agent's relationship with the Participant terminates.

4.11.3 Prior to disclosing information to an Agent, the Agent must enter into a written agreement with Healthix that includes, but is not limited to, the following:

a. A specific statement that the Agent is working on behalf of the Participant, and a commitment to notify Healthix if the Agent is no longer working on behalf of the Participant;

b. Confirmation that the Agent has entered into a Business Associate Agreement with Participant, if required by applicable law;

c. A specific statement that the Agent may only use or disclose Protected Health Information obtained from Healthix on behalf of the Participant and for those purposes that the Participant would be permitted to use or disclose the Protected Health Information, subject to any limitations in the Business Associate Agreement between the Participant and the Agent;

d. An obligation for the Agent to implement security measures to safeguard Protected Health Information in a manner meeting or exceeding the minimum security requirements (i) of a Business Associate under HIPAA and (ii) as specified in a Participant Agreement;

e. A requirement for Agent to report to Healthix any Breach, security incident or unauthorized use or disclosure of Protected Health Information obtained from Healthix; and

f. Agent's indemnification of Healthix.

4.11.4 An employee of an Agent is not eligible to be an Authorized User, and therefore, the Agent may receive information from Healthix, but may not access the Healthix computer system.

SECTION 5: PATIENT ENGAGEMENT AND ACCESS

Purpose/Principles

This Section 5 sets forth minimum requirement Healthix and its Participants shall follow to ensure that patients are able to understand what information exists about them, how that information is used, and how they can access such information,

Policies and Procedures

5.1 **Patient Education**. Healthix shall 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 inform 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 Healthix.

5.1.1 Healthix shall provide, or shall require their Participants to provide, at the time affirmative consent is obtained, 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 Healthix; (ii) terms and conditions upon which their Protected Health Information can be shared with Authorized Users; (iii) the benefits and risks of providing Affirmative Consent (iv) a complete, accurate and updated list of Healthix Data Suppliers; (v) information about how to contact Data Suppliers; (vi) a description of how patients may deny consent for Participants to Access their Protected Health Information through Healthix; (vii) information about how patients can submit requests to correct erroneous data; (viii) information about how patients can submit requests for Audit Logs; and (ix) information about the security practices of the SHIN-NY, including the right of patients to be notified of certain breaches and how data sent outside the SHIN-NY upon a patient request may no longer be subject to HIPAA.

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

5.2 **Patient Access to Protected Health Information**. To the extent permitted or required by law, Healthix shall provide patients and their Personal Representatives, if applicable, with access to the patients' Protected Health Information that is maintained by Healthix through one of the mechanisms set forth in Sections 5.2.1(a), (b) or (c) below.

5.2.1 Each patient or his or her personal representative, as applicable, shall have the right to indicate the scope of the Protected Health Information and which of the mechanisms below he or she prefers to utilize to obtain access to the Protected Health Information, and, except as otherwise set forth herein, Healthix shall abide by the patient's, or personal representative's, request unless applicable law (including the patient access provisions under the HIPAA Privacy Rule or the requirements for the "content and manner"

exception or another exception to the Information Blocking Rules) permit or require Healthix to limit the scope and form of the Protected Health Information provided to the patient or personal representative. The mechanisms through which Protected Health Information may be obtained include:

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

b. A paper or electronic copy of information maintained about the patient by Healthix

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

5.2.2 Healthix shall only facilitate such access after confirming the identity of the patient or the patient's Personal Representative through adequate identity proofing procedures.

5.2.3 For minors who are less than ten (10) years of age, Healthix will permit parents and guardians with access to their minor children's Protected Health Information as set forth in this Section 5.2. For minors at or over ten (10) years of age, Healthix will not provide parents or guardians with access to a minor child's Protected Health Information and will instead refer parents and guardians of such minors to the applicable Participants for access to a minor's Protected Health Information. Healthix will provide minors at or over ten (10) years of age with access to their own Protected Health Information as set forth in this Section 5.2.

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

5.3.1 Healthix shall Disclose the patient's Protected Health Information in response to the patient's or Personal Representative's request only after confirming the identity of the patient or the patient's Personal Representative that submitted the request through adequate identity proofing procedures.

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

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

5.3.4 Healthix may require a patient, a patient's Personal Representative, or a third party to pay a fee prior to Disclosing Protected Health Information to a third party only if applicable law, including the patient access provisions under the HIPAA Privacy Rule and the Information Blocking Rule, permit such fee to be charged.

5.4 **Patient Education**. Healthix and its Participants shall participate in any applicable patient education programs developed by the State Designated Entity through the SCP for the purpose of educating patients about the uploading of their Protected Health Information to Healthix.

5.5 [Left intentionally blank]

5.6 **Requests to Correct Erroneous Information.**

5.6.1 QEs shall direct patients to the appropriate Participants who can assist them in a timely fashion to resolve an inquiry or dispute over the accuracy or integrity of their Protected Health Information, and to have erroneous information corrected or to have a dispute documented if their request to revise data is denied.

5.6.2 Each QE shall require its Participants and Data Suppliers to notify the QE if, in response to a request by a patient, the Participant or Data Supplier makes any corrections to the patient's erroneous information.

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

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

5.7 **Patient Participation in Decision Making**. Healthix shall develop a plan and process for assuring meaningful patient/consumer input and participation in Healthix operations and decision making.

5.8 Informing Patients About Access. As required in Section 6.4, Healthix shall require its Participants to provide patients with information about how their Protected Health Information was accessed through Healthix.

5.9 Providing patients the option to withhold information. Participants may, but shall not be required to, provide patients the option to withhold patient information, including minor consent information, from Healthix. Participants that choose to provide patients with this option must document the patient's decision and not transmit the patient information to Healthix.

SECTION 6: AUDIT

Purpose/Principles

This Section 6 sets forth minimum requirement that Healthix and its Participants shall follow when logging and auditing access to health information via Healthix.

Policies and Procedures

6.1 **Maintenance of Audit Logs.** Healthix shall maintain Audit Logs that document all access of Protected Health Information via Healthix.

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

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

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

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

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

6.1.3 Other Requirements Regarding Audit Logs and Access

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

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

6.1.4 Other Requirements Regarding Audit Logs and Transmittals

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

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

6.1.5 General Audit Log Requirements

a. Audit Logs shall be immutable. An immutable Audit Log requires either that log information cannot be altered by anyone regardless of access privilege or that any alterations are tamper evident. This provision will take effect when the necessary functionality is deployed in the new Healthix system or when QE certification commences, whichever is sooner. Certified Applications must also comply with this provision.

b. 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 Reviews. Healthix shall conduct, or shall require each of its Participants to conduct, periodic reviews to monitor use of Healthix 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, Healthix shall review, or require its Participants to review, the following:

a. That Affirmative Consents are on file for patients whose Protected Health Information is accessed via Healthix, other than in Break the Glass situations;

b. That Authorized Users who access Protected Health Information via Healthix do so for Authorized Purposes;

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

d. That applicable requirements were met where Protected Health Information was accessed through a One-to-One Exchange; and

e. That applicable requirements were met where Protected Health Information was accessed through a One Time Override.

6.2.2 If a Participant accesses Protected Health Information via Healthix through a Certified Application, the reviews 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 Healthix's Participants shall be reviewed.

6.2.4 Periodic reviews shall be conducted at least on an annual basis. In addition, reviews shall occur

a. Following a Breach that involves serious deviation from these Policies and Procedures;

b. In response to a patient complaint involving Protected Health Information obtained via Healthix; and

c. When concerns regarding a Participant's use of Healthix are identified by Healthix.

Healthix 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 reviews more often than annually. Notwithstanding the foregoing, all Break the Glass incidents shall be reviewed.

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

6.2.6 If reviews are conducted by Participants rather than by Healthix, the Healthix shall:

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

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

6.3 Participant Access to Audit Logs.

6.3.1 Healthix shall provide the Participant, upon request, with the following information regarding any patient of the Participant whose Protected Health Information was accessed via Healthix:

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 Healthix 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 Healthix shall provide patients, upon request, with the following information:

a. The name of each Participant that accessed a 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.).

6.4.2 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, Healthix and that Participant shall take the following actions:

a. Healthix 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 Healthix 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 for its Authorized User access and determines that all of the Authorized User(s) accessed the patient's information for Authorize 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 2 access the patient's information for Authorized Purposes, the Participant shall (i) inform the patient of this finding; (ii) provide the patient with the name(s) of the Authorized User(s) who inappropriately accessed the patient's information unless the Participant has a reasonable belief that such disclosure could put the Authorized User at risk of harm, in which case the Participant shall provide the patient with an opportunity to appeal this determination to a representative who is more senior to the individual(s) who made the original determination; and (iii) inform Healthix of the inappropriate access and otherwise comply with the requirements of Section 7.

6.4.3 If requested, Participants will provide such information to patients at no cost once in every 12-month period. Healthix and/or its Participants may establish a reasonable fee for any additional requests within a given 12-month period; provided that 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 Healthix.

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

6.5 Public Availability of Audits. Healthix shall make the results of its periodic reviews available on the Healthix 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 review.

6.6 Correction of Erroneous Data. In the most expedient time possible and without unreasonable delay, Healthix 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 Healthix data aggregation and exchange activities and, if an error is determined to exist, identify the root cause of the error and ensure its correction. Healthix shall log all such errors, the actions taken to address them and the final resolution of the error. Healthix 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.** Healthix shall require weekly confirmation by Organ Procurement Organizations that all instances in which Protected Health Information was accessed through Healthix by the Organ Procurement Organization's Authorized Users were consistent with the terms of these Policies and Procedures (based upon a listing sent by Healthix).

6.8 **Additional Requirements Related to Auditing of Public Health Access.** Healthix shall use special safeguards with respect to audits of access by Public Health Agencies, which shall include at least the following:

6.8.1 Healthix 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 Healthix 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, Healthix may suspend all Authorized User accounts associated with that particular workgroup until the situation is resolved.

SECTION 7: BREACH

Purpose/Principles

This Section 7 sets forth minimum standards Healthix and its Participants shall follow in the event of a breach. They are designed to hold violators accountable for violations, assure patients about Healthix commitment to privacy, and mitigate any harm that privacy violations may cause. Healthix Incident Response Plan (Appendix C) provides procedural guidance in the event of a privacy or security incident.

Policies and Procedures

7.1 Obligation of Participants to Report Actual or Suspected Breaches. Participants shall notify Healthix in the event that a Participant becomes aware of any actual or suspected Breach involving Protected Health Information accessed via Healthix.

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.

7.1.3 Healthix will monitor all Breaches involving 500 or more individuals reported by Participants to DHHS via Office of Civil Rights on a regular basis but no less than monthly, and in accordance with its internal procedure.

7.2 Responsibilities of Healthix.

7.2.1 Healthix will require all of its subcontractors who have access to Protected Health Information to inform Healthix in the event of a suspected Breach.

7.2.2 In the event Healthix becomes aware of any suspected Breach, either through notification by a Participant or subcontractor or otherwise, Healthix shall 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.

7.2.3 In the event it is determined that an actual Breach has occurred, Healthix shall:

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 Healthix or the Participant. Healthix mitigation efforts shall correspond with and be dependent upon its internal risk assessment.

c. Except as set for in Section 7.2.3(d), require the Participant whose information was exposed to arrange for the applicable notifications as

required by HIPAA/HITECH and State law. If another Participant or Business Associate of a Participant was the cause of the Breach, the involved Participants and/or Business Associates may decide to delegate the notification requirements to the extent permitted under applicable law. Participants or Business Associates, which cause a Breach of another Participant's Protected Health Information, are encouraged to accept responsibility for the Breach notifications.

d. If Breach was specifically caused by Healthix' breach of its Business Associate responsibilities, including unauthorized access or disclosure by a Healthix employee, be responsible to make the notifications required under HIPAA/HITECH and State law.

7.2.4 Notwithstanding the foregoing, neither Healthix nor Participant shall be required to make a report otherwise required by this Policy if a law enforcement agency investigating a Breach request that Healthix or the Participant refrain from notifying any other party of the Breach.

7.2.5 In the event that it is determined that the suspected Breach is not an actual Breach, Healthix will document (or require the applicable Participant to document) a risk assessment that describes why there is a low probability that Protected Health Information was compromised.

7.2.6 Healthix will record each and every report received, the investigation undertaken, and the disposition, if any. Healthix will also keep records, or require the Participant to keep records, of any sanctions imposed for a violation of Healthix Policies, any employees, agents or contractors involved, and any further action taken, including sanctions against workforce members.

7.3 Liability for Breaches. Healthix will accept liability for Breaches when the Breach or results from Healthix' or Healthix staff's acts or omissions (e.g., security mechanisms on the Healthix that do not prevent an unauthorized access). Each Participant shall be liable for Breaches that result from acts or omissions by that Participant's staff members. Authorized Users that are not affiliated with a Participant shall be liable for their own Confidentiality Breaches or unauthorized access.

SECTION 8: COMPLIANCE

Purpose/Principles

While it is anticipated that most Participants will be Covered Entities and thus subject to the HIPAA Privacy Rule and HIPAA Security Rule, there may be some Participants that are not Covered Entities. The provisions of this Section 8 are designed to ensure that entities accessing Protected Health Information through Healthix 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 **Covered Entities.** Each Participant that is a Covered Entity shall comply with the HIPAA Privacy Rule and HIPAA Security Rule.

8.2 **Non-Covered Entity Participants.** Each Participant that is not a Covered Entity, other than a public health authority or a health oversight agency as defined by HIPAA , that receives Protected Health Information shall assess whether addressable safeguards under the HIPAA Security Rule should be adopted. In determining which addressable safeguards to adopt, such Participants shall take into account their size, complexity, capabilities, and other factors set forth under 45 C.F.R Section 164.306(b). Nothing herein shall be construed to require Participants to comply with the HIPAA Security Rule and HIPAA Privacy Rule with respect to information that does not constitute Protected Health information.

8.3 **HIPAA Officers.** Healthix shall identify a Privacy Officer and a Security Officer who shall be responsible for ensuring compliance with the applicable HIPAA provisions.

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

8.4.1 A Community Based Organization that is not a Covered Entity may not Access Protected Health Information via the SHIN-NY and instead may only receive Transmittals of Protected Health Information via direct or another encrypted means of communication.

8.4.2 Healthix may Transmit Protected Health Information to a Community Based Organization that is not a Covered Entity only if

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

b. The Transmittal meets the requirements of One-to-One Exchange under Section 1.2.1 or is a Patient Care Alert that meets the requirements of Section 1.2.10 and the Transmittal occurs in compliance with the HIPAA Privacy Rule and any other applicable federal laws

8.4.3 Healthix shall undertake reasonable efforts to limit the Protected Health Information Transmitted to a Community Based Organization that is not a Covered Entity to the minimum amount necessary to accomplish the intended purpose of the Transmittal, taking into account the nature of the Community Based Organization receiving the Transmittal, the reason(s) such organization has requested the Protected Health Information, and other relevant factors.

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

SECTION 9: SANCTIONS

Purpose/Principles

Sanctions are an important mechanism for ensuring that Participants and Authorized Users comply with these Policies & Procedures. The provisions in this Section 9 are designed to provide guidelines for the imposition of sanctions Healthix and its Participants.

Policies and Procedures

9.1 **Identification.** Upon report of a complaint, regarding use of or access to the Healthix, Breach, or other violation of the Healthix Policies, Healthix shall so inform the applicable Participant.

9.2 **Participant Policies**. Participants are required to have sanctions policies that are consistent with this Section 9.

9.3 **Non-Intentional/Minor Violations.** If it is identified that an Authorized User has unintentionally violated the Healthix Policies, or the violation is minor, in most circumstances, the Participant can impose discipline/sanctions in accordance with its routine policies.

9.4 **Intentional, Egregious or Substantial Violations.** If an intentional, egregious or significant violation of Healthix Policies or applicable law is identified, the Healthix Board may impose sanctions in addition to any sanctions imposed by the relevant Participant. The proposed Healthix Board action should be to review the proposed sanction with the Participant prior to imposing such sanction, unless immediate action is necessary to protect Healthix.

9.5 **Bases for Sanctions.** When determining the type of sanction to apply, Healthix and/or their Participants shall take into account the following factors: (a) whether the violation was a first time or repeat offense; (b) the level of culpability of the Participant or Authorized User (e.g., whether the violation was made intentionally, recklessly or negligently); (c) whether the violation constitutes a crime under state or federal law; and (d) whether the violation resulted in harm to a patient or other person.

9.6 **Sanctions.**

9.6.1 Sanctions that may be imposed by Healthix include:

a. Written warning;

b. Temporary restriction on use of Healthix;

c. Required re-education;

d. Permanent termination as an Authorized User of Healthix;

e. Suspending or terminating a Participant's participation in Healthix;

f. The assessment of fines or monetary penalties; or

g. Report to regulatory agencies or law enforcement.

9.7 **Documentation**. All sanctions and disciplinary actions relating to Healthix shall be documented in the Healthix Sanction Log and documentation maintained for six (6) years.

9.8 **Training**. Participants and Public Health Agencies shall inform all Authorized Users about the Healthix sanctions policies.

SECTION 10: EMERGENCY ACCESS/DISASTER RECOVERY

Purpose/Principles

Healthix and all Participants shall have in place an information systems data and backup recovery plan and disaster recovery/emergency mode operation plan consistent with HIPAA requirements and applicable law. These include: (a) data backup plan to establish and implement procedures to create and maintain retrievable exact copies of Protected Health Information; (b) disaster recovery plan to establish and implement as needed procedures to restore any loss of data; an emergency mode operation plan to establish and implement as needed procedures to enable continuation of critical business processes and protection of the security of electronic protected health information while operating in emergency mode.

Policies and Procedures

10.1 Applications and Data Criticality Analysis.

10.1.1 Each Participant shall perform an assessment of the criticality, vulnerability and security of its programs and information that are part of Healthix. This assessment shall be kept reasonably current to reflect changes in the Participant's technical infrastructure including, but not limited to, the introduction of new systems and/or security features or a change in criticality to the operation of the Participant. Documentation of such assessment shall be maintained by the Participant and may be requested by, and provided to, Healthix as necessary for Healthix to ensure compliance with these policies.

10.1.2 Healthix shall maintain a current assessment of criticality, vulnerability and security of the Healthix infrastructure for which Healthix is responsible.

10.2 Data Back-up Plan. Healthix shall ensure that Healthix or its vendors backs-up the relevant components of Healthix. Such back-ups shall be maintained in a separate location from the applicable hardware and shall be immediately available in the event of an emergency in which the emergency mode operation plan is initiated.

10.3 Disaster Recovery Plan

10.3.1 Each Participant will implement a disaster recovery plan that allows for timely restoration of its functionality within the Healthix whenever possible.

10.3.2 In the event of a fire, vandalism, natural disaster or system failure, Healthix will take the following measures to restore lost data:

a. In the event of a system failure where the system cannot be restored to minimal functionality or if the system is otherwise not operational, Healthix will retrieve the most current back-up media from the offsite location(s) identified above.

b. In the event of a system failure or if the computer system is only partially operational, Healthix will attempt to resolve the issue internally. If it

cannot, it will contact the relevant software vendor or other entity with which it has a maintenance contract to restore any lost data.

10.4 Emergency Mode Operation Plan

10.4.1 In the event of fire, vandalism, natural disaster or system failure affecting the Participant's computer component necessary for the Participant to participate in Healthix, Participant shall take steps to either (a) obtain its backup tapes and operate as part of the Healthix from a remote location; or (b) operate independently using its main servers, without connecting to the Healthix System. In the event that the latter option is implemented, the Participant shall inform Healthix regarding the situation.

10.4.2 In the event of a system failure or if Healthix is only partially operational, Healthix will attempt to resolve the issue internally. If it cannot, it will contact the relevant software vendor or other entity with which it has a maintenance contract to restore the functionality of the system.

a. In the event of a system failure where Healthix cannot be restored to minimal functionality or if the system is otherwise not operational, Healthix or its vendor (e.g., the hospital services vendor) will retrieve the most current back-up diskettes from the off-site location and operate from a contractually agreed upon location (the hosting services vendor will be responsible for establishing such contractual location).

10.5 Testing and Revisions

10.5.1 Participants shall routinely test their Disaster and Emergency Mode Operation Plans and, upon request of Healthix, provide documentation to Healthix regarding such testing.

10.5.2 On at least an annual basis, Healthix will arrange for a test of Healthix disaster recovery capabilities with regard to the individual servers, databases or portions of systems supporting services to Participants.

SECTION 11: PRIVACY AND SECURITY GOVERNANCE

Purpose/Principles

Healthix shall establish policies and procedures for the operation of Healthix

Policy and Procedure

11.1 Proposed Policies. The Healthix President & CEO, Senior Director of Compliance, or Chair of the Audit and Compliance Committee, Technical Manager, a Healthix Board member, or any Privacy and Security Committee member may recommend additions or amendments to these Policies and Procedures. After review and discussion with the Healthix Privacy and Security Committee, the Chair of the Healthix Privacy and Security Committee will make a recommendation to the Healthix Board regarding each such new proposed policy. All new policies must be approved by the Healthix Board and take effect 45 days after notifying Participants of the updated policies, unless otherwise approved by the Healthix Board. The Healthix President & CEO shall be responsible for ensuring that Participants are informed of substantive revisions to the Healthix Policies.

11.2 Committee Review. The Healthix President & CEO will ensure that the Healthix Privacy and Security Committee meets on a regular basis and shall assure that policies are reviewed as needed.

11.3 Local Policies. Privacy and Security Officers at Participant or vendor organization are responsible for implementation and enforcement of the policies and procedures applicable to their specific organizations.

Version Control

Version Number	Date revision approved by Privacy Committee	Summary of Change	Revised By/Date Accepted by Healthix Board
1.0 – 5.0		Document creation - Legacy Documents and subsequent Updates	Garfunkel Wild/Healthix Board on 03.04.2014 – 12.19.2018
6.0	2.25.2019	Policy Revisions § 1.9.3 (Multiparticipant consent form), Policy Revisions § 1.7.2 (Use of PHI for Patient Recruitment for Research), § 1.6.1.c (Access by Healthix to de-identified or limited data sets to advise study team about of identifying sufficient potential subjects)	Garfunkel Wilde/Board Approved on 3.21.2019
7.0	05.07.2020	Policy Revisions § 1.2.1 (1:1 Exchange), § 1.2.11 (Death Notifications), § 1.2.12 (Disclosures to Death Investigators) §1.9.18 (Transmittals to Non-Participants) § 1.13 (Transmittals to Other Participants), §3.2 Authentication Requirements, §3.5 Authentication of Certified Application s and Downstream users, § 6.1.2 Audit Logs and Transmittals, Appendix A (User role table),	M. Mandzielewska & Garfunkel Wilde/Board Approved on 6.03.2020

Version Number	Date revision approved by Privacy Committee	Summary of Change	Revised By/Date Accepted by Healthix Board
		appendix B (SHIN-NY Guidance for Authentication Requirements)	
8.0	7.29.20	Policy Revisions §1.13 (Life and Insurance disability)	M.Mandzielewska & Garfunkel Wild/Board Approved on 9/02/2020
9.0	11.07.2020	Policy Revisions §1.9.13 (Restrictions on Disclosures to Payers)	M.Mandzielewska & Garfunkel Wild/Board Approved on 3/24/2021
	02.01.2021	Policy Revisions § 1.2.12 (Payer Access for HEDIS/QUARR), §1.2.13 (Telehealth) § 5.2.1-4, 5.3, 5.4 (Patient Engagement and Access), §7.2.3 c&d (Breach Notification), § 8.4 (CBOs)	
10.0	06.29.2021	Policy Revisions § 1.2.2 (1:1 Exchange), § 5.2.1 – 5.2.3 & 5.3 (Patient Engagement and Access), § 12.1-12.8 (Patient Portal)	M.Mandzielewska & Garfunkel Wild/Board Approved on 10/06/2021
	09.09.2021	Policy Revisions § 1.2.4 (Break-The-Glass), § 1.2.12 (Death Notifications), § 5.1-5.6 (Patient Engagement and Access	
11.0	1.21.2022	Policy Revisions § 1.3.5 Naming of QE and Recognition of Consents	M.Mandzielewska/ Board Approved on 03/09/2022
12.0	5/12/2022	Policy Revisions: Added version control, revised Section 1, Section 4, Section 5 and Section7 Add Appendix C – Healthix Incident Response Plan.	Garfunkel Wild/Board Approved on 06/08/22
13.0	5/12/2023	Policy Revisions: Added definition of Centralized Research Committee and Social Services Program. Revised the following policy Sections: 1.2.3 (f), 1.5.1, 1,7,4, 1.13.6 and 8.2 and 8.4	M.Mandzielewska & Garfunkel Wild/. Approved by Healthix Board 6/06/23
14.0	12/05/2023 03/19/2024 06/04/2024	Policy Revisions: Added Definition for: Health Oversight Agency. Revised Definitions for: Social Services, Emergency Medical Technician and Patient Care Alerts. Added Provision 1.2.16 Health Oversight Agencies, and Section 1.14 Waivers During Public Health Emergency Revised Provision 1.2.1 One-to-One Exchanges	M.Mandzielewska & Garfunkel Wild. Approved by Healthix Board 6/05/24

Appendix A

Authorizers Users – Role Based Access Standards

Category	Access Authority	Role	Types of User (e.g.)
Practitioner, Authorized User under direction of Practitioner, Advanced Medical Technician with temporary rights to access PHI – Break Glass	• Break the Glass Authority • All clinical information and functionality (and any non-clinical information)	• Physician – Commonly engaged in providing emergency care	• MD who routinely provides care that could require "Break the Glass" emergency access to RHIO data
		• Resident	• Resident • Fellow
		• Physician Assistant Commonly engaged in providing emergency care	• Physician Assistant who routinely provides care that could require "Break the Glass" emergency access to RHIO data
		• Nurse Practitioner Commonly engaged in emergency care	• Nurse Practitioner who routinely provides care that could require "Break the Glass" emergency access to RHIO data
		• Nurse Midwife	• Nurse Midwife
		• ED Nurse	• ED Nurse (RN)
		• Emergency Medical Provider (EMTs)	• EMS
Practitioner – No Break Glass	• All clinical information and functionality (and any non-clinical information)	• Physician - Not commonly engaged in providing emergency care	• MD who does NOT routinely provide emergency care (this may apply to private practice physicians)
		• Physician Assistant Not commonly engaged in providing emergency care	• PA who does NOT routinely provide emergency care (this may apply to practice Physician Assistants)
		• Nurse Practitioner Not commonly engaged in providing emergency care	• NP who does NOT routinely provide emergency care (this may apply to private

Category	Access Authority	Role	Types of User (e.g.)
			practice Nurse Practitioners)
		• Nurse	• Nurse (RN) • LPN
		• Therapists (licensed)	• Respiratory Therapists • Rehabilitation Therapists
		• Pharmacists	• Pharmacists
		• Psychologist	• Psychologist
		• Nutritionist	• Nutritionist • Dietician
		• Care/Case Managers (licensed)	• Care Manager • Social Worker (clinical)
Non-Practitioner – Clinical Information (and any non-clinical information)	• All clinical information and functionality (and any non-clinical information)	• Stakeholder Administration • Care/Case Managers (unlicensed) • Therapists (unlicensed)	• Clinician Office Staff • Quality Assurance • Intake Planner • Discharge Planner • Social Worker Assistant • Care Navigator
	• Limited clinical information, including Demographics and Advanced Directives and any non-clinical information)	• Patient Representative	• Patient Representative • Patient Advocate • Patient Navigator • Ombudsman
Non-Practitioner – No Clinical Information	• NA		
RHIO Admin – Clinical Information (and any non-clinical information)	• Break the Glass Authority • All clinical information and functionality (and any non-clinical information) • Audit logs and report	• RHIO Administrative Staff – Data Rights	• RHIO Administrative Staff (specifically identified)
RHIO Admin – No Clinical Information	• Audit logs and report	• RHIO Administrative Staff	• RHIO Administrative Staff

Category	Access Authority	Role	Types of User (e.g.)
RHIO Admin – Clinical Information for Public Health Reporting or other authorized activities	• All clinical information and functionality • Audit logs and report	• RHIO Administrative Staff	• RHIO Administrative Staff
RHIO or Participant Admin –Clinical Information (and any non-clinical information)	• All clinical information and functionality (and any non-clinical information) • Audit logs and report	• RHIO Administrative Staff • Participant Administrative Staff	• RHIO Administrative Staff • Participant Administrative Staff
Tester (confidentiality agreement necessary)	• Own clinical information	• Stakeholder Technical/QA Staff	• Stakeholder Staff (specifically identified)
Public Health	• All Demographic and Clinical Data except 42 CFR Part 2	• Public Health Agency	• Public Health Agency Staff
Death Investigator	• All Demographic and Clinical data except OMH and OPWDD	• Coroner/Medical Examiner	• Coroner/Medical Examiner

APPENDIX B

SHIN-NY Policy Guidance for Authentication Requirements as per the Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State (V3.7 and V3.6) issued April 4th, 2020.

Section 3: Authentication

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 policy guidance sets forth the minimum requirements that QEs and their participants shall follow when authenticating individuals prior to allowing them access to information via the QE Clinical Viewer as well as the exceptions to authentication requirements for EHRs and System-to-System applications otherwise referred to in SHIN-NY Policies and Procedures as Certified Applications.

1. QEs shall authenticate, and/or shall require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Authenticator Assurance Level 2 (AAL2) set forth in National Institute of Standards and Technology Special Publication 800-63 (hereinafter, "NIST SP 800-63") for the QE Clinical Viewer.

2. QEs may authenticate EHRs and System-to-System applications using the Authentication Requirements found in SHIN-NY P&Ps version 3.6 which states that 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 ("Level2") set forth in NIST Special Publication 800-63. 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. QEs may institute a Trusted Site Program which allows Participants to apply to become an approved Trusted Site. The value of a Trusted Site is that users who have successfully authenticated to the Trusted Site's network will not require use of a second factor to access the clinical information and services available through the QE. In the case of a Trusted Site, the second factor is now accounted for through the source IP address of the end user.