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:

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

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

Affiliated Practitioner means (i) a Practitioner employed by or under contract to a 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) a consent mechanism approved by NYS DOH as an alternative to a Level 1 Consent or a Level 2 Consent under Section 1.3; or (iv) a consent that may be relied upon under the Patient Consent Transition Rules set forth in Section 1.8.2.

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

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.

Authorized User means an individual who has been authorized by a Participant or Healthix to access patient information through 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 QE can demonstrate that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the Protected Health Information or to whom the disclosure was made; (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 a QE or Participant, if such acquisition, access, or use was made in

good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; (ii) any inadvertent disclosure by a person who is authorized to access Protected Health Information at a QE or Participant to another person authorized to access Protected Health Information at the same QE or Participant, or organized health care arrangement in which a Participant participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or (iii) a disclosure of Protected Health Information where a QE or Participant has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Break the Glass means the ability of an Authorized User to access a patient's Protected Health Information without obtaining an Affirmative Consent in accordance with the provisions of Section 1.2.3.

Business Associate Agreement means a written signed agreement meeting the HIPAA requirements of 45 CFR § 164.504(e).

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

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.

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

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

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 satisfies the requirements of 45 C.F.R. § 164.514(b).

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

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.

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 Consent means the Level 1 consent form developed by the New York State Medicaid Program to allow Health Homes access to a QE.

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

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

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

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

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

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

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

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

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, mental health or substance abuse treatment) or services consented to by an Emancipated Minor.

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

Organ Procurement Organization (OPO) means a regional, non-profit organization responsible for coordinating organ and tissue donations at a hospital that is designated by the Secretary of Health and Human Services under section 1138(b) of the Social Security Act (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, Health Home or Health Home Member, PPS, 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 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 Consent Transition Rules means the rules set forth in Section 1.8.

Payment means the activities undertaken by (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or (ii) a health care provider or health plan to obtain or provide reimbursement for the provision of health care. Examples of payment are set forth in the HIPAA regulations at 45 C.F.R. § 164.501.

Payer Organization means an insurance company, health maintenance organization, employee health benefit plan established under ERISA or any other entity that is legally authorized to provide health insurance coverage.

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 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.

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.

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

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

Protected Health Information means individually identifiable health information (e.g., any oral or recorded information relating to the past, present, or future physical or mental health of an individual; the provision of health care to the individual; or the payment for health care) of the type that is protected under the HIPAA Privacy Rule.

Provider Organization means an entity such as a hospital, nursing home, home health agency or professional corporation legally authorized to provide health care services.

Public Health Agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, 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 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.

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

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

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

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 means the single entity that: (1) has been designated by the Governor as eligible to receive from the federal government state grants to promote health information technology and conforms to federal requirements to receive such awards, or that has been certified by the Commissioner of Health as meeting the requirements of 10 N.Y.C.R.R. Part 300; (2) is a not-for-profit entity that includes on its board of directors representation from a broad range of SHIN-NY stakeholders; (3) demonstrates that its principal purpose is to serve the people of the State of New York by using information technology to create and maintain the SHIN-NY; and (4) adopts nondiscrimination and conflict of interest policies that demonstrate a commitment to open, fair, and nondiscriminatory participation by SHIN-NY stakeholders.

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.

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.

SECTION 1: CONSENT

Purpose/Principles

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 1.7.5

1.2 Exceptions to Affirmative Consent Requirement. Notwithstanding anything to the contrary set forth in this Section, Affirmative Consent shall not be required under the circumstances set forth below:

1.2.1 One-to-One Exchanges. Affirmative Consent shall not be required for a Participant to access a patient's Protected Health Information via Healthix from another Participant in a One-to-One Exchange provided the Participants comply with existing federal and state laws and regulations requiring patient consent for the disclosure and re-disclosure of information by health care providers. [1]

1.2.2 Public Health Reporting and Access.

a. A Public Health Agency may access Protected Health Information through Healthix clinical viewer or portal for the following public health purposes without Affirmative Consent:

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

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

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

iv. To investigate suspected or confirmed cases of lead poisoning (pursuant to 10 N.Y.C.R.R. § 67-2.3); or

v. For other public health purposes authorized by law and approved through the Statewide Collaboration Process and by the Healthix Board.

[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.

b. 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 2.2.2(a)(i)-(v).

c. 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.

1.2.3 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 Advanced 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 Advanced Emergency Medical Technician's judgment, an emergency condition exists and the patient is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the patient's life or health.

ii. The Practitioner or Advanced Emergency Medical Technician determines, in his or her reasonable judgment, that information that may be held by or accessible via 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 Advanced Emergency Medical Technician is affiliated.

iv. In the event that an Authorized User acting under the direction of a Practitioner Breaks the Glass, such Authorized User must record the name of the Practitioner providing such direction. 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, Advanced Emergency Medical Technician or Authorized User acting under the direction of a Practitioner attests that all of the foregoing conditions have been satisfied, and the 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 Section 1.1.1(h) of these Policies and Procedures. In lieu of providing such notice, Participants that are hospitals may notify all patients discharged from an emergency room that their 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.

1.2.4 **Converting Data.** Affirmative Consent shall not be required for the conversion of paper patient medical records into electronic form or for the uploading of Protected Health Information from the records of a Data Supplier to 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.

1.2.5 **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.

1.2.6 De-Identified Data. Affirmative Consent shall not be required for access to De-identified Data for specified uses as set forth in Section 1.6.

1.2.7 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

1.3 Form of Patient Consent. Except as otherwise permitted by the Patient Consent Transition Rules set forth at Section 1.8, consents shall be obtained through an Approved Consent. Healthix and/or its Participants (after prior coordination with Healthix) may request approval from NYS DOH to use a consent other than a Level 1 Consent or Level 2 Consent. Such approval will not be granted unless the alternative consent is substantially similar to the Level 1 Consent or Level 2 Consent, as applicable, and achieves the same basic purposes as such consents, as set forth in these Policies and Procedures. 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 approved by NYS DOH under Section 1.3. All consents must include the following information:

a. The information to which the patient is granting the Participant access, including specific reference to HIV, mental health, alcohol and substance abuse, reproductive health, sexually-transmitted disease, and genetic testing information;

b. The intended uses to which the information will be put by the Participant;

c. The relationship between the Participant and the patient whose information will be accessed;

d. A list of or reference to all Data Suppliers at the time of the patient's consent, as well as an acknowledgement that Data Suppliers may change over time and instructions for patients to access an up-to-date list of Data Suppliers through 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 from a QE website or by other means;

e. Certification that only those engaged in Level 1 Uses may access the patient's information;

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

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

h. The time period during which the consent is to be effective;

i. The signature of the patient or the patient's Personal Representative; and

j. The date of execution of the consent.

1.3.2 Level 2 Uses. Consent to access information via Healthix for the purposes of Level 2 Uses shall be obtained using a Level 2 Consent or an alternative consent approved by NYS DOH. All consent for Level 2 uses shall include (i) the information required of a Level 1 Consent pursuant to Section 1.3.1 and (ii) the following:

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

b. Whether 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.

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 NYS DOH.

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 PHR 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 Healthix and its Particpants will permit the exchange of information about minors other than Minor Consent Information based on an Affirmative Consent executed by the minor's Personal Representative.

1.5.2 A Participant may access Minor Consent Information through Healthix based on an Affirmative Consent executed by the minor's Personal Representative unless federal law or regulation requires the minor's authorization for such disclosure, in which case a Participant may not access such information without the minor's Affirmative Consent.

1.5.3 Notwithstanding section 1.5.2, Healthix and its Participants may not disclose Minor Consent Information 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 1.5.3.

1.5.4 Sections 1.5.1 through1.5.3 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.

1.5.5 Neither Healthix nor its Participants shall exchange of 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.

1.6.1 Access of De-Identified Data for Specified Uses. Affirmative Consent shall not be required for a Participant or a government agency to access De-Identified Data via Healthix for the following purposes:

a. Research approved by an Institutional Review Board organized and operating in accordance with 45 C.F.R. § 164 and Section 1.6.4 below; or

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

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

1.6.3 Other Requirements.

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

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

c. 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.

1.6.4 Additional Research Requirements.

a. De-identified Data obtained through Healthix can be accessed, used or disclosed for research purposes provided the following conditions are met:

i. The applicable data must be de-identified in accordance with the requirements of HIPAA.

ii. The research applicant must meet the qualifications to be an Authorized User.

iii. The Healthix Board shall designate a subcommittee (For purposes of this Section, the "Subcommittee") to approve applications under this Section.

iv. The specific use as permitted in this Section must approved by the Subcommittee.

b. In order to request Healthix approval for access, use or disclosure of De-Identified Data for a research purpose, an application must be submitted to the Subcommittee. 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);

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 information 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 applicant's Participant organization);

ix. Dissemination plan (i.e., the intended use of the results of the study, including 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); and

xiii. A statement that the researcher agrees to comply with all Healthix policies.

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

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

e. 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.

f. Healthix will establish a standard fee schedule to use De-identified Data for research, 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.

g. 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 Subcommittee prior to proceeding with the revisions.

h. Investigators are prohibited from:

   i. combining the Healthix De-identified Data with any other source without prior approval by Healthix;

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

   iii. 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 Subcommittee and the identifiable participant have granted prior approval for such presentation or dissemination;

   iv. sharing De-identified Data with any individual who is not a member of the investigation team as listed on the original application or approved modification;

   v. using De-identified Data for purposes other than those expressly described in the original application and approved modification.

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

j. All De-identified Data shall be returned to Healthix or destroyed at the end of the approved study period.

k. Healthix will periodically inform Participants of ongoing research projects.

1.7 Other Policies and Procedures Related to Consent.

1.7.1 Affiliated Practitioners. An Affirmative Consent obtained by a Participant shall apply to an Affiliated Practitioner of the Participant provided that (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.

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

1.7.3 Consents Covering Multiple Participants. An Affirmative Consent may apply to more than one Participant provided that the consent (a) lists each Participant with sufficient specificity to provide reasonable notice to the patient as to which Participant may access the patient's information Healthix pursuant to such consent and (b) provides the patient with the option to select which of the Participants listed on the consent may access the patient's information via Healthix. 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.

1.7.4 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.

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

1.7.6 Denial of Consent. Consents shall give the patient the option of granting or affirmatively denying consent for individual Participants to access information about the patient via 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.

1.7.7 Durability. An Affirmative Consent for Level 1 Uses does not have to be time-limited. An Affirmative Consent for Level 2 Uses shall be time-limited and shall expire no more than two years after the date such Level 2 Consent is executed, except to the extent a longer duration is required to complete a Research protocol.

1.7.8 Revocability. Patients shall be entitled to revoke an Affirmative Consent at any time provided that such revocation shall not preclude any Participant that has accessed Protected Health Information via 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.

1.7.9 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.

1.7.10 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.

1.7.11 Disclosure to 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.

1.7.12 Compliance with Existing Law. All access to Protected Health Information 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.

1.7.13 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 f 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 of 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.

1.7.14 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.

1.7.15 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.

1.7.16 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.

1.7.17 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.

1.8 Patient Consent Transition Rules.

1.8.1 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.

1.8.2 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.

1.9 Receipt of Patient Care Alerts.

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

1.9.2 Patient Care Alerts containing Protected Health Information shall be sent in an encrypted form that complies with U.S. Health and Human Services Department Guidance to

Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

SECTION 2: AUTHORIZATION

Purpose/Principles

Authorization is the process of determining whether a particular individual within a Participant has the right to access Protected Health Information via 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. Non-Practitioner with access to clinical and non-clinical information;

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

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

f. 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

g. 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 5.4.8; 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.

3.2.1 Authentication Standard. Until such time as a determination is made, pursuant to Section 3.2.2, to utilize a higher authentication standard, QEs shall authenticate, or shall requite their Participants to authenticate, each Authorized Uses through an authentication methodology that meets the minimum technical requirements for Identity Level of Assurance 2 ("Level 2") set forth in National Institute of Standards and Technology Special Publication 800-63 (hereinafter, "NIST SP 800-63").

Level 2 will require, among other technical specifications, Healthix or its 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, Healthix or its 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 Healthix 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 Healthix.

3.2.2 Transitional Authentication Standard., Upon notification by NYeC, Healthix shall authenticate, or require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum requirements for Identity Level of Assurance 3 ("Level 3") set forth in NIST SP 800-63.

a. Level 3 will require, among other technical specifications, Healthix or its Participants to authenticate each Authorized User's identity using multifactor authentication, which queries Authorized Users for something they know (e.g., a password) *and* something they have (e.g., an ID badge or a cryptographic key). Healthix and its Participants may use a combination of tokens (authentication secrets to which an Authorized User's identity is bound), including soft

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

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

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 Section 3 of these Policies and Procedures.

SECTION 4: ACCESS

Purpose/Principles

Access controls govern when and how a patient's information may be accessed by Authorized Users through 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 (e.g., the probability of success of an online password guessing attack shall not exceed 1 in 16,384 over the life of the password).

4.1.3 Group or temporary user names shall be prohibited.

4.1.4 Authorized Users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing passwords.

4.1.5 Authorized Users shall be prohibited from sharing their user names and/or passwords with others and from using the user names and/or passwords of others.

4.1.6 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 hall 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 1.7.1.

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.

5.2 **Patient Access to Protected Health Information**. Healthix shall, or shall require its Participants to, develop and educate patients and/or their Personal Representatives with respect to policies related to patients' rights to access their own Protected Health Information. At the current time, Healthix does not provide patients and/or their Personal Representatives with access to their own Protected Health Information, and therefore, Healthix shall inform patients and/or their Personal Representatives that may access the patients' Protected Health Information by contacting their health care providers.

5.3 **Patient Notice**. Healthix shall require their Participants to provide, patients with (i) notice — in a manner easily understood by patients — that their Protected Health Information is being uploaded to Healthix; (ii) a list of or reference to all Data Suppliers (consistent with Section 1.7.9); (iii) information about how to contact Data Suppliers; and (iv) a description of how patients may deny consent for all Healthix Participants to access their Protected Health Information through Healthix in accordance with Section 1.7.6. 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.

5.4 [Left intentionally blank]

5.5 **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.

5.6 **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.

5.7 **Patient Inquires about Accuracy of Information**. Healthix 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.

5.8 Patient Corrections. Participants and Data Suppliers are required to notify Healthix if, in response to a request by a patient, the Participant or Data Supplier makes any corrections to the patient's erroneous information.

5.9 Informing Patients about Participant Access to Erroneous Information. Healthix shall make reasonable efforts to provide its Participants with information indicating which other Healthix Participants have accessed erroneous information that the Participant has corrected at the request of patients in accordance with Section 5.7.

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

6.1.3 With respect to access to Protected Health Information through Healthix 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. 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.

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

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

6.2 Obligation to Conduct Periodic 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; and

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

6.2.2 If a Participant accesses Protected Health Information via 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 assist its Participants to provide patients, upon request, with the following information:

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

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

c. The time and date of such access; and

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

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

6.4.3 If requested, 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.

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.

7.2 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 their internal risk assessment.

c. Require the Participant whose information was exposed to notify the patient and any applicable regulatory agencies as required by and in accordance with applicable federal, state and local laws and regulations, including but not limited to HITECH.

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 requests 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: HIPAA COMPLIANCE

Purpose/Principles

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

8.2 Each Participant that is not a Covered Entity shall adopt all of the applicable administrative, physical and technical safeguards set forth in the HIPAA Security Rule as well as the restrictions on the use and disclosure of Protected Health Information set forth in the HIPAA Privacy Rule.

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

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 of 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

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.

Attachment 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 BHIX 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 BHIX data
		• Nurse Practitioner Commonly engaged in emergency care	• Nurse Practitioner who routinely provides care that could require "Break the Glass" emergency access to BHIX 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 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	• Patient Representative	• Patient Representative • Patient Advocate • Patient Navigator

	Advanced Directives and any non-clinical information)		• 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
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)