HEALTHCARE INFORMATION XCHANGE OF NEW YORK, INC.,
doing business as Hixny

DATA EXCHANGE
POLICIES AND PROCEDURES

APPROVED BY BOARD OF DIRECTORS
May 15, 2017

Table of Contents

Definitions

Capitalized terms appearing in these Policies and Procedures shall have the following meanings:

- **Access Event** means an activity that occurs during the accessing of patient information from the RHIO, such as, for example, patient search, patient summary access, etc.

- **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 Data Recipient to render health care services to the Data Recipient's patients; (ii) a Practitioner on a Data Recipient's formal medical staff; or (iii) a Practitioner providing services to a Data Recipient's patients pursuant to a cross-coverage or on-call arrangement.

- **Affirmative Consent** means the consent of a patient obtained through the patient's execution of (i) the Hixny Patient Consent Form, or (ii) an alternative mechanism of consent approved by the New York State Department of Health.

- **Associated Hardware** means the servers and network equipment Hixny has acquired and installed at both the central Hixny facility and at Participant sites.

- **Associated Software** means the software that is required to utilize the Associated Hardware as well as the application software required to provide the Services that comprise the System.

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

- **Authorized User** is an individual Data Recipient or an individual designated to access the System and use the Services on behalf of the Data Recipient, including without limitation an employee or independent contractor of the Data Recipient, a credentialed member of the Data Recipient's medical staff, or the member(s) or owner(s) of a physician organization that is a Data Recipient who are authorized by Data Recipient to access the System and use the Services on behalf of the Data Recipient, who has executed the standard Hixny Authorized User Form.

- **Breach** means the acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI. A Breach is presumed unless it can be demonstrated that there is a low probability that PHI has been compromised based on a risk assessment of certain factors outlined in the Breach Policy. Breach excludes:
    i. an unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of Hixny or a 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 PHI at Hixny or a Participant to another person authorized to access PHI at Hixny or the same 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 PHI where Hixny or a 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.

- **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 Payor Organization to determine whether coverage should be extended or Payment should be made for health care service.

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

- **Data Provider** is a Participant that is registered to make health information accessible to other Participants through the System and Services.

- **Data Recipient** is a Participant whose Authorized Users use the System and Services to access health information.

- **De-Identified Data** is data that does not identify the individual and with respect to which there is no reasonable basis to believe that the information can be used to identify the individual. Data shall be considered de-identified if it satisfies HIPAA's requirements for De-Identified data, as defined in 45 CFR Section 164.514(b). **Disaster Relief Agency** means (i) a government agency with authority under federal, state or local law to declare an Emergency Event or assist in locating individuals during an Emergency Event or (ii) a third party contractor to which such a government agency delegates the task of assisting in the location of individuals in such circumstances.

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

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

- **Health Care Agent** means an adult to whom authority to make health care decisions has been delegated by a patient via a health care proxy form in accordance with Article 29-C of the Public Health Law.

- **HIPAA** means the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations promulgated thereunder, including 45 CFR Parts 160 and 164, as amended (such regulations herein referred to as the "HIPAA Privacy Rule").

- **Hixny Patient Consent Form** means the standard consent form developed by the NYS Department of Health that must be executed by a patient before a Data Recipient may access the patient's health information via the System.

- **Hixny Data Exchange Policies and Procedures** means the policies and procedures contained within this document, as adopted by the Hixny Board of Directors.

- **Hixny Withdrawal of Consent Form** means the standard revocation form developed by Hixny that must be executed by a patient in order for the patient to revoke his/her consent to a particular Data Recipient or all Data Recipients to access the patient's health information.

- **Insurance Coverage Verification** means the use of information by a Participant, other than a Payor Organization, to determine which health plan covers the patient or the scope of the patient's health insurance benefits.

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

- **Marketing** has the meaning ascribed to this term under the HIPAA Privacy Rule as amended by Section 13406 of HITECH.

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

- **Participant** means a party that is registered with Hixny and will either act as a Data Provider or Data Recipient, or both.

- **Personal Representative** means a person who has the authority to consent to the disclosure of a patient's Protected Health Information under Public Health Law § 18 and any other applicable State or Federal laws and regulations, including the following: (i) a guardian for an incapacitated person appointed under Article 81 of the Mental Hygiene Law; (ii) a parent of an infant or a guardian of an infant appointed under Article 17 of the Surrogate's Court Procedure Act or other legally appointed guardian of an infant who may request access to a clinical record; (iii) a distributee of any deceased subject for whom no personal representative, as defined in the Estates, Powers, and Trusts Law, has been appointed; or (iv) an attorney representing a qualified person or the subject's estate explicitly authorizing the holder to execute a written request for patient information.

- **One-to-One Exchange** means a disclosure of Protected Health Information by one Participant to one or more other Participants, where (a) the receiving Participant is either treating the patient or performing Quality Improvement and/or Care Management activities for such patient, and (b) no records other than those of the Participants jointly providing health care services to the patient are exchanged. Disclosure of such PHI is controlled by the sender Participant in compliance with all applicable laws and regulations. Such exchanges of PHI are understood and predictable to the patient because they mirror currently accepted paper-based or other information exchange business practices that are controlled by the sending Participant and, thus, such exchanges do not require additional consent from the patient to the receiving Participant.

- **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.

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

- **Practitioner** means a health care professional licensed under Title 8 of the New York Education Law or a resident or student acting under the supervision of such a professional.

- **Protected Health Information** or **PHI** 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.

- **Quality Improvement** means conducting quality measurement, assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities related to improving health and reducing health care costs, evaluating Practitioner and provide performance, clinical decision support tools, evidence-based clinical protocol development, case management and care coordination, and contacting of healthcare providers and patients with Treatment alternatives and related functions.

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

- **Sensitive Health Information** means certain health information that is specially protected under New York and/or Federal laws, rules and regulations and for which special requirements apply to the disclosure of such information. Such information includes, but is not limited to, HIV/AIDS, mental health, alcohol and substance abuse, reproductive health, sexually-transmitted disease, and genetic testing information.

- **Services** shall mean the information-sharing Services available to Participants through the System, as more fully described in the Hixny Data Exchange Policies and Procedures.

- **SHIN-NY** means a set of agreements (and the transactions, relations and data that are created by and through such set of agreements) entered into to make possible the statewide 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.

- **System** means the secure, network-based peer-to-peer computer system owned and operated by Hixny that allows clinicians and other users to access aggregated patient clinical data held by multiple health care organizations which may have disparate health information computer applications.

- **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** or **Unsecured PHI** means PHI 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) of HITECH. For purposes of these policies and procedures, Unsecured PHI shall mean PHI that is accessed via the System.

Hixny Data Recipient – Privacy and Security Requirements Policy

Policy Number	**L4000**
Policy Description	**This policy describes the privacy and security requirements that Hixny places on Data Recipients using the System and Services.**
Policy Intent	**To ensure that Hixny data is appropriately protected within the Data Recipient's own environment.**
Applies to	**All Data Recipients accessing Protected Health Information from Hixny.**
Original Policy Date	**9/15/2008**
Revision History	**10/15/2010**

Principles

1. Hixny Data Recipients will conform to federal and NYS requirements with regard to allowable uses of the System by the Authorized Users granted access to the System by the Data Recipients.
2. Within the constraints of federal and NYS requirements and law and the Participation Agreement, each Data Recipient will determine how the System is be used within its own environment.
3. Data Recipients are responsible for the security of data accessed from the System after that data enters the Data Recipient's own environment.
4. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Data Recipient Privacy and Data Security

    a. Within its own environment, each Data Recipient must afford the data accessed from the System and Services the same level of security, privacy and access control that the Data Recipient affords all other confidential health information.
        i. Each Data Recipient shall refer to and comply with its own internal policies and procedures that apply to the access, use, and disclosure of Sensitive Health Information that is accessed from the System and Services.

    b. Each Data Recipient must ensure that its internal policies and procedures that control the access to, use of, and disposition of Personal Health Information (PHI) also apply to data accessed from the System while such data exists within the Data Recipient's own internal environment.

    c. Each Data Recipient will comply with the HIPAA Privacy Rule with respect to any PHI accessed from the System and Services.

d. Each Data Recipient must grant Hixny the right to review its applicable internal policies and procedures, in order for Hixny to verify that such policies and procedures provide for appropriate control over PHI that is accessed from the System and Services. New Data Recipients must submit to Hixny a certification attesting that they have an internal Data Security Policy that complies with HIPAA requirements and any other requirements as determined by Hixny.

e. Data Recipient shall require that all Authorized Users comply with the internal policies and procedures of the Data Recipient with regard to data accessed from the System and Services.

f. Data Recipient shall ensure that its internal policies and procedures regarding access, use and disclosure of PHI accessed from the System and Services comply with applicable Federal and State laws and regulations and the Participation Agreement.

Hixny Participant Requirements Policy

Policy Number	**L4100**
Policy Description	**This policy describes the requirements that Hixny Participants must comply with in order to be allowed continued use of the Hixny System and Services.**
Policy Intent	**To ensure that Data Providers and Data Recipients comply with the same policies, procedures and processes in both providing data to the System and accessing data from it.**
Applies to	**All Participants who wish to either provide Protected Health Information to Hixny or access patient health information from Hixny.**
Original Policy Date	**9/15/2008**
Revision History	**10/15/2010, 3/13/2015**

Principles

1. Hixny will require a minimum set of information regarding each Data Recipient's Authorized Users in order to add these Authorized Users to the System. It will be the Data Recipient's responsibility to provide such information.
2. An Authorized User of the System must have reasonable confidence that s/he is viewing as complete a set of clinical data as is available.
3. An Authorized User of the System must have reasonable confidence that s/he is viewing as accurate a set of clinical data as is possible.
4. For mutual and individual protection, both Hixny and the Participant shall obtain and maintain insurance coverage in commercially reasonable amounts.
5. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Data Provider Responsibilities

   a. In order to ensure completeness of information, and consistent with New York State guidelines, Data Providers will send the data elements designated by Hixny into the System for all patients, even if such information is considered Sensitive Health Information and is specially protected by New York State or Federal law.
   b. Each Data Provider will take reasonable measures to ensure the accuracy of the data submitted to the System. This will include, at a minimum, taking steps as deemed appropriate by the Data Provider to ensure that the data sent to the Hixny System is an accurate reflection of the data that exists in the Data Provider's own electronic health record ("EHR") system at the time such data is made accessible through the System.

i. When correcting any inaccuracies in their own EHR System, Data Providers must also take appropriate and reasonable measures to ensure that the correction is accurately reflected in the Hixny System.

ii. Each Participant shall notify Hixny if, in response to a request by a patient, the Participant makes any corrections to the patient's erroneous information. Hixny will take reasonable efforts to provide such Participant with information indicating which other Participants may have accessed erroneous information that the Participant has corrected at the request of a patient.

ii. Each Data Provider shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information. If as a result of a patient request, the Data Provider accepts an amendment to the health information about the patient, the Data Provider shall make reasonable efforts to ensure that the amendment is accurately reflected in the Hixny System.

2. Data Recipient Responsibilities

a. Trusted Agent Designation: Each Data Recipient shall appoint at least one "Trusted Agent". Trusted Agents shall be nominated by the authorized signer of the Hixny Participation Agreement or other executive officer within the Data Recipient's organization. The Data Recipient acknowledges and agrees that it is fully responsible for the Trusted Agent's compliance with the responsibilities below. Trusted Agents shall be responsible for:
   i. Designating who from their organization will be deemed an Authorized User.
   ii. Verifying that each Authorized User meets the Identity Proofing requirements listed in 2.c.
   iii. Countersigning Authorized User Agreements.
   iv. Acknowledging that all Authorized User information provided to Hixny is accurate, current and complete.
   v. Working with Hixny on the Authorized User account reconciliation process defined in 2.o.
   vi. Working with Hixny representatives to help facilitate any Data Recipient related audits defined within these policies and procedures.

b. Authorized User Information. Upon designating an individual to be an Authorized User of the System, the Data Recipient must provide Hixny with the following information in order for system access to be granted:

   i. First Name
   ii. Last Name
   iii. Email Address
   iv. Clinical Data Access Group
   v. Used Class
   vi. Proxy To User Id (required if proxy access is requested)
   vii. DEA Number (required if the Authorized User will use the e-prescribing functionality)
   viii. Attestation that the appropriate Authorized User Agreement has been executed
   ix. Any other information requested by Hixny

c. Authorized User Identity Proofing Requirements. Each Data Recipient shall:
   i. Identity Proofing Requirements: Prior to each potential Authorized User requesting an account the Trusted Agent shall require each user account applicant to provide name, address, date of birth, and a valid government issued photo ID. The Trusted Agent shall:

a. inspect the government issued photo ID;
b. compare the picture on the government issued photo ID to the applicant and verify that they appear to be the same person; and
c. verify that the name, address, date of birth and government issued photo ID number on the photo ID for the applicant are the same as those reflected in the records of (i) the applicable agency or institution issuing the photo ID (e.g., Department of Motor Vehicles), (ii) e-Verify, or (iii) a credit bureau (e.g., Equifax, Experian or TransUnion). If the Trusted Agent is unable to verify the applicant's name, address, date of birth, or government issued photo ID number, the Trusted Agent shall refuse to verify or authenticate the identity of the applicant.

ii. Changes to Identity Proofing Requirements: The identity proofing procedures may be changed upon reasonable advance notice.

iii. The Data Recipient shall maintain records of the identity verification process, including (i) each applicant's name, address, date of birth, government issued photo ID type and number, (ii) name of Trusted Agent performing identity proofing, (iii) date and time verification performed, and (iv) source used to perform verification (e.g., DMV, e-Verify, credit bureau).
   a. The Data Recipient must securely retain the records of identity verification for seven years after the applicant ceases to be employed by, associated with, authorized by, or affiliated with the Data Recipient. Hixny may, at any time and from time to time, audit any or all applicant identity verification records, and Data Recipient shall ensure that, upon reasonable advance notice, Hixny will be provided with access to such records.

iv. Data Recipient shall abide by Termination of Access policy listed in 2.n.

v. Data Recipient shall re-verify the identity of any given Authorized User if the Data Recipient becomes aware of information that calls into question the validity the Authorized User's information is not, or is no longer, accurate or current (e.g., due to a name change or move). The Data Recipient shall promptly notify Hixny of such change.

d. User IDs. Data Recipient must recognize that designating an individual to be an Authorized User of the System may not result in the assigning of a new User ID to that individual. If the designee is an individual who has already been granted access by another Data Recipient, Hixny will expand his/her access rights to include patients of the new Data Recipient, but will not issue a second user ID.

e. Access. Each Data Recipient shall allow access to the System only by individuals designated as Authorized Users who have a legitimate and appropriate need to obtain information from Hixny. No Authorized User shall be provided with access to the System without first having been trained on these Policies, as set forth below. Before access is granted, each Authorized User must sign the Hixny Authorized User Agreement and each Data Recipient must make the certifications required in Section 5.3 of the Participation Agreement.

f. Training. Each Data Recipient shall develop and implement a training program for its Authorized Users to ensure compliance with these Policies. The training shall include a detailed review of applicable Policies and each trained Authorized User shall sign the Authorized User Agreement, which states that he or she received, read, and understands all applicable Policies and has completed all training required by Participant. Data Recipients shall maintain the Hixny Authorized User Agreements for a minimum of six (6) years. Upon Hixny's request, Data Recipient shall make available a record of who has received training.

g. Disciplinary Procedures. Each Data Recipient shall implement procedures to discipline and hold Authorized Users, work force members, agents, and contractors accountable for ensuring that they do not use, disclose, or request health information except as permitted by these Policies and that they comply with these Policies. Such discipline measures shall include, but not be limited to, verbal and written warnings, demotion, and termination, or termination of contractual relationships or restriction or termination of privileges, where applicable, and provide for retraining where appropriate.

h. Reporting Non-Compliance. Each Data Recipient shall have a mechanism for, and shall encourage, all Authorized Users and other workforce members, agents, and contractors to report any non-compliance with these Policies internally. Further, each Data Recipient shall ensure that any such non-compliance reported internally is promptly reported to Hixny. Each Data Recipient also shall establish a process for individuals whose health information is included in the System to report any non-compliance with these Policies or concerns about improper disclosures of information about them.

i. Notification to Hixny of Certain Events. Each Participant shall notify Hixny upon the occurrence of any incident or report involving illness, injury, death, property damage or other loss related to the use of or access to the System or the SHIN-NY.

j. Mitigation. Each Data Recipient shall implement a process to mitigate, and shall mitigate and take appropriate remedial action, to the extent practicable, any harmful effect that is known to the institution of a use or disclosure of health information obtained through the System or Services in violation of applicable laws and/or regulations and/or these Policies by the institution, its Authorized Users, or its workforce members, agents, and contractors. Steps to mitigate could include, among other things, Data Recipient notification to the individual of the disclosure of information about them or Data Recipient request to the party who received such information to return and/or destroy the impermissibly disclosed information.

k. Disclosures of PHI. Each Data Recipient shall ensure that all disclosures of PHI through Hixny and the use of information obtained from Hixny shall be consistent with all applicable federal, state, and local laws and regulations, including but not limited to, the HIPAA Privacy Rule, and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to accessing health information, the Data Recipient shall be responsible for obtaining the required documentation or meeting the requisite conditions. Data Recipient shall comply with all applicable federal, state and local laws and regulations regarding the re-disclosure of health information obtained through Hixny.

l. Minimum Necessary. Each Data Recipient shall limit its Authorized Users access to PHI through the System to the minimum amount necessary to accomplish the intended purpose for which the information is accessed and only for those purposes that are permitted by applicable federal, state, and local laws and regulation, the Participation Agreement, and these Policies. The limitation on the minimum amount necessary does not apply when PHI is accessed for Treatment purposes only.

m. Permissible Use of the System. Use of the System by Data Recipients for any purpose other than Treatment and Quality Improvement and Care Management, and Insurance Coverage Verification is prohibited.

n. Accounting of Disclosures. Each Data Recipient that discloses health information obtained through Hixny shall document the purposes for which such disclosures are made, and any other information that may be necessary for compliance with the HIPAA Privacy Rule's accounting of disclosures requirement. Each Data Recipient is responsible for ensuring its compliance with such requirement and may choose to provide individuals with more information in the accounting than is required. Hixny shall provide audit information that may be required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement as needed.

o. Termination of Access. Data Recipient shall notify Hixny within one business day of termination of an Authorized User's or Trusted Agent's employment or affiliation with the Data Recipient. In the event that the sole Trusted Agent is terminated, the Data Recipient shall appoint a new Trusted Agent or the duties will default to the signatory of the Participant Agreement. Hixny shall terminate the account for a terminated user within one business day of Data Recipient notification. In the event a Data Recipient

cancels its participation with Hixny, Hixny shall terminate all user accounts associated with the Data Recipient within one day of notice from the Data Recipient.

p. Authorized User Account and Trusted Agent Reconciliation: Hixny may on an annual basis or as deemed necessary, perform an Authorized User account and/or Trusted Agent reconciliation. Each Data Recipient shall be responsible for working with Hixny to identify individuals whose accounts or status need to be terminated or modified.

q. Hixny's Sanctions: Hixny, at its sole discretion, will have the right to impose sanctions for any violation of this policy. Please refer to Hixny's Sanction Policy, Policy L4800.

3. Participant Responsibilities: Insurance

a. During the term of the Participant Agreement, each Participant shall procure and maintain comprehensive general liability insurance with limits of at least one million dollars ($1,000,000) per occurrence and two million dollars ($2,000,000) in the aggregate.

b. Each Participant shall notify Hixny immediately of the existence of any claims or events that might result in any claim or claims against Hixny, Participant and/or an Authorized User by virtue of any act or omission on the part of Participant or an Authorized User in its use of the System or Services. Each Participant shall comply with any reasonable request by Hixny for disclosure of information concerning such claim or event as required by Hixny or any insurance carrier of Hixny and shall cooperate in providing such disclosure even in the event that the Participation Agreement should terminate for any reason.

Hixny System Responsibilities Policy

Policy Number	**L4200**
Policy Description	**This policy describes Hixny and Participant's technical responsibilities with respect to the implementation and ongoing operation of the System and Services.**
Policy Intent	**To ensure that the ongoing technical obligations of Hixny and each Participant regarding the System and Services are documented and agreed upon.**
Applies to	**Hixny and its subcontracting vendors, where applicable.**
Original Policy Date	**_____/2010**
Revision History	**10/15/2010, 3/13/2015**

Principles

1. Hixny will administer the System and Services in a professional and effective manner so that System availability and System response times comply with commercially reasonable standards.
2. Hixny will work with new Participants to promote a smooth implementation of the System.
3. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Hixny/Participant System Responsibilities – Implementation

   a. In order to add a new Participant to the System, Hixny's responsibilities are as follows:
      i. Acquire and provide appropriate hardware (server and network equipment) to allow the new Participant's data to be stored and accessed.
      ii. Install the appropriate portions of the Associated Software on that hardware, including the interface software that receives the data from the Participant and properly stores it for access.
      iii. If requested, provide training for key staff from the Participant, allowing that staff to then assume responsibility for further Participant training.

      For any hardware or software acquired by Hixny, Hixny shall retain title to and ownership of such products and shall have the right to install, maintain and inspect such products.

   b. In order to become a new Participant to the System, a Participant's responsibilities are as follows:
      i. Acquire and/or develop the interfaces necessary to transmit the data from the Participant EHR system to the Hixny System.
      ii. Validate that these interfaces correctly transmit this data to the System and that the System displays this data correctly, accurately and completely.

iii. Participate with Hixny in the testing required to ensure that the new Participant's data is being correctly integrated with existing Participant data within the System.
iv. Comply with such other requirements as determined by Hixny.

c. Training: All Authorized Users of each Data Recipient shall be responsible for completing training requirements for educating individuals about the policies and procedures for accessing Protected Health Information.
i. Before gaining access to the Hixny System each Authorized User is required to complete either on-site training, web-based training, or comparable training tools so that Authorized Users are familiar with the operation of Hixny and the policies and procedures governing access to information via the SHIN-NY governed by Hixny.
ii. Participants shall be required to complete such training prior to being granted access to information via Hixny.
iii. Each Authorized User shall be required to certify that he or she has received training and will comply with the Hixny's policies and procedures. Such certification may be made on a paper form or by electronic attestation and shall be retained by Hixny or Participants for at least six years.
iv. Authorized Users are required to complete HIPAA training on an annual basis. Participants will be required to demonstrate compliance by completing an attestation that the annual HIPAA training has been completed by all Authorized Users.

2. Hixny System Responsibilities – Ongoing

a. Subject to subsection (g) below, Hixny will use reasonable efforts to ensure that malfunctions of either the Associated Hardware or the Associated Software are repaired on a timely basis. If a Participant discovers a malfunction, the Participant will notify Hixny of the existence of the malfunction in a timely manner. Participant will also use reasonable efforts to provide documentation to assist Hixny in addressing the malfunction with its vendors. Hixny will respond to notifications of malfunctions from its Participants in a timely manner, and will exert reasonable effort toward their resolution.

b. Subject to subsection (g) below, Hixny will use reasonable efforts to ensure that enhancements to either the Associated Hardware or the Associated Software are implemented on a timely and routine basis. Hixny will develop a schedule for the implementation of any such non-critical changes and/or enhancements, and will publish that schedule to all Participants. Hixny will use reasonable efforts to maintain all elements of the System at the levels of currency required for continued vendor support.

c. Hixny will provide ongoing day-to-day user support through a central Help Desk that may be accessed either by phone or by email. Participants have the option of having their users either call the Hixny Help Desk directly or having their users contact their own internal Help Desk first, with that Help Desk contacting the Hixny Help desk if necessary.

d. Hixny will routinely provide audit information to Participants, detailing accesses to patient clinical information by that Participant's Authorized Users. Each Participant is responsible for review of this information to identify any inappropriate access. Upon the specific request of Hixny, Participant shall confirm to Hixny that such a review has been completed.

e. Hixny may, from time to time, offer additional reports to Participants regarding areas of interest, provided that these reports fall within the accepted uses of the data (Treatment and quality assurance). Participants may request a specific report of interest from Hixny, but Hixny, at its sole discretion, will determine if the requested report is to be provided.

f. Hixny must comply with all NYS and Federal law concerning the release of the confidential information that is housed within the System. Hixny will not release information to any government agency unless (i) it is compelled to do so by NYS or Federal law or by court order, (ii) a Participant so requests in writing, or (iii) as otherwise permitted in accordance with Hixny Data Exchange Policies and Procedures. If Hixny is required to release information for any reason other than subsection (iii), Hixny will notify all Data Providers that submitted such information of the requirement to release the information prior to the actual release of the information.

g. Notwithstanding the foregoing, Hixny shall not be responsible for malfunctions of the Associated Hardware or Software, delays in the implementation of enhancements, delays in providing support, or the adequacy or timeliness of any corrections, repairs or other Services provided by any third party service providers where such malfunctions, delays, or inadequate corrections, repairs or Services are not the direct result of the negligent acts or omissions or willful misconduct of Hixny.

3. Hixny Responsibilities - Insurance

a. During the term of the Participant Agreement, Hixny shall procure and maintain comprehensive general liability insurance with limits of at least one million dollars ($1,000,000) per occurrence and two million dollars ($2,000,000) in the aggregate.

b. Hixny shall notify each Participant immediately of the existence of any claims or events that might result in any claim or claims against Participant and/or a Participant's Authorized User by virtue of any act or omission on the part of Hixny, Participant or an Authorized User in its use of the System or Services. Hixny shall comply with any reasonable request by Participant for disclosure of information concerning such claim or event as required by Participant or any insurance carrier of Participant and shall cooperate in providing such disclosure even in the event that the Participation Agreement should terminate for any reason.

Hixny Services Policy

Policy Number	**L4300**
Policy Description	**This policy describes the information-sharing Services Hixny offers to Data Recipients.**
Policy Intent	**To ensure clarity among Data Recipients with regard to the Services to be provided by Hixny as well as the permitted and prohibited use of these Services.**
Applies to	**All Data Recipients wishing to access patient health information from Hixny.**
Original Policy Date	**9/15/2008**
Revision History	**10/15/2010, 3/13/2015**

Principles

1. Hixny will conform to NYS law and requirements with regard to allowable uses of the System by the Authorized Users granted access by the Data Recipients.
2. Hixny will provide a common, consistent set of Services to all Data Providers and Data Recipients within the constraints imposed by NYS requirements and law.
3. Within the constraints of NYS requirements and law, each Data Recipients may determine how the System may be used within its own environment.
4. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Hixny Services

   a. Hixny will provide the Authorized Users of each Data Recipient access to the System. Assuming patient consent has been obtained in accordance with the Hixny Patient Consent Policy, the System will provide the following information-sharing Services (collectively, the "Services"):
      i. Matching of patients based on facility Medical Record Number or probabilistic matching based on patient demographic information. Hixny will endeavor to provide the most effective matching possible within the constraint of avoiding any matching of different patients. During the search process, Hixny will also utilize technical restrictions to minimize the display of patient information to avoid incidental disclosure of demographic PHI of non-consenting patients.
      ii. A list of the clinicians within Data Providers from whom the patient has received care, the role of that clinician (attending, consulting, etc.), the date of that interaction, and, minimally, the chief complaint for which the patient sought that care.
      iii. A list of known allergies for that patient.
      iv. A history of the medications prescribed for or given to the patient by the clinicians within the Data Providers.

v. A list of the prescriptions filled by the patient, obtained from nationally recognized sources (RxHub and SureScripts).
vi. The Medical Record Number that is used to store that patient's information within other Data Provider EHR systems.
vii. Next of kin information for that patient that may have been provided by another Data Provider.
viii. Other patient specific clinical information as determined by Hixny with the endorsement of the Hixny Clinical Committee.

b. Hixny shall, at its sole discretion, assign a new Authorized User to one of the following existing roles within the System:
i. Break the Glass - a (1.) Practitioner; (2.) Authorized User acting under the direction of a Practitioner; or (3.) Advanced Emergency Medical Technician who, by law has temporary rights to access Protected Health Information for a specific patient.
ii. Practitioner with access to clinical and non-clinical information.
iii. Non-Practitioner with access to clinical and non-clinical information.
iv. Non-Practitioner with access to non-clinical information.
v. QE Administrator with access to non-clinical information.
vi. QE Administrators with access to clinical information in order to engage in Public Health.
vii. QE or Participant Administrators with access to clinical and non-clinical information for purposes of system maintenance and testing, troubleshooting and similar operational and technical support purposes.

c. Hixny shall provide Data Recipients with an Audit Log documenting which Authorized Users accessed information about which patients and when such information was accessed. Hixny shall also work towards implementing a system wherein, upon request, patients have an on line means to display which Authorized Users have accessed information about them through the System and when such information was accessed.

d. The Hixny System shall provide re-disclosure warning statements to Authorized Users whenever they access the following types of records:
i. Records of federally-qualified alcohol or drug abuse programs regulated under 42 C.F.R. Part 2. The warning statement should include the language required by 42 C.F.R. § 2.32.
ii. HIV/AIDS information protected under Article 27-F of the New York Public Health Law. The warning statement should include the language required by Article 27-F.
iii. 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. The warning statement should contain language indicating that such records may not be re-disclosed except as permitted by the New York State Mental Hygiene Law.

e. The Hixny System is compliant with HIPAA's technical and administrative standards and the SHIN-NY Statewide Collaboration policies, including but not limited to the following:
i. Authentication of the identity of Authorized Users;
ii. Use of unique user names and passwords;
iii. 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);
iv. Group or temporary user names shall be prohibited;
v. Authorized Users shall be required to change their passwords at least once every 90 calendar days and shall be prohibited from reusing passwords;
vi. 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;

vii. Limits on failed access attempts. Upon a fifth failed access attempt Authorized User accounts will be locked out until access is restored by Hixny;

viii. Termination after periods of inactivity.

Hixny requires that any other system used for authentication and access to the System also complies with such standards.

f. Hixny may permit Certified Applications to access PHI in accordance with the terms of Hixny's Policies and Procedures, provided that the credentials of any Certified Application requesting access to PHI or the System be properly authenticated. As a condition of granting such access, Hixny shall require a Participant using a Certified Application to provide Hixny with (i) the name and contact information of the individual responsible for requesting access through the Certified Application on the Participant's behalf and (ii) a certification signed by such individual acknowledging that he or she is personally responsible for the use of the Certified Application for this purpose. The Participant shall be required by the QE to update this information and provide a new certification prior to changing the individual responsible for the use of the Certified Application.

g. Hixny shall require a Participant using a Certified Application to limit access to any PHI 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 Hixny's Policies and Procedures if they were accessing PHI directly through Hixny.

h. Hixny reserves the right to change, modify or terminate the Services at any time, subject to Board approval and the requirements of the Participation Agreement.

2. Use of the Services

a. All disclosures of health information through Hixny and the use of information obtained from Hixny shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to accessing health information, the Data Recipient shall be responsible for obtaining the required documentation or meeting the requisite conditions. Data Recipient shall comply with all applicable federal, state and local laws and regulations regarding the re-disclosure of health information obtained through Hixny.

b. A Data Recipient may request health information from the System only for purposes permitted by applicable law. Each Data Recipient shall request health information from the System only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and regulation, the Participation Agreement, and these Policies.

c. As defined by the Participation Agreement, use of the System by Data Recipients is limited to Treatment and Quality Improvement and Care Management, and Insurance Coverage Verification purposes only.

d. Each Data Recipient that discloses health information obtained through Hixny shall document the purposes for which such disclosures are made, and any other information that may be necessary for compliance with the HIPAA Privacy Rule's accounting of disclosures requirement. Each Data Recipient is responsible for ensuring its compliance with such requirement and may choose to provide individuals with more information in the accounting than is required. Hixny shall provide audit information that may be required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement as needed.

Hixny Patient Consent Policy

Policy Number	**L4400**
Policy Description	**A Data Recipient must receive a patient's affirmative and informed written consent before the Data Recipient's Authorized Users can access the patient's Protected Health Information on the System, unless an exception applies.**
Policy Intent	**To ensure that patients provide affirmative, informed and written consent to have their PHI accessed by a Data Recipient's Authorized Users in accordance with Federal and State laws, rules and regulations and any contractual arrangements between Hixny and New York State.**
Applies to	**All Data Recipients who wish to access a patient's Protected Health Information.**
Original Policy Date	**9/15/2008**
Revision History	**Revised 10/13/08 to reflect changes in consent requirements for minors; 01/__/2011 (Data Provider Access); 11/2/2012 (references to BTG Policy), 3/13/15 (Consent Audit and Sanctions); 7/13/2015 (One to One exchange definition, new exceptions to disclosures,);**

Principles

1. New York State law requires hospitals, physicians, other health care providers, and payors obtain patient consent before disclosing Protected Health Information for non-emergency Treatment.
2. RHIOs, such as Hixny, are required to obtain written consent from patients before a Data Recipient's Authorized Users access any Protected Health Information, unless an exception applies.
3. This policy is intended to set forth a standardized procedure to be followed by all Data Recipients for obtaining patient consent in order for a Data Recipient's Authorized Users to access the patient's Protected Health Information via the System.
4. This policy addresses accessing a patient's Protected Health Information only for the purposes of Treatment, Quality Improvement and Care Management, and Insurance Coverage Verifications, in accordance the Hixny Data Exchange Policies and Procedures. It does not address patient consent related to Research (unless De-Identified Data) or Marketing uses.
5. Hixny may modify this policy from time to time with Board approval.

Procedures

1. General Considerations

   a. Unless an exception described in Section 7 applies, a Data Recipient must obtain a patient's affirmative and informed written consent before the Data Recipient's Authorized Users may access the patient's Protected Health Information via the System.

   b. An Affirmative Consent obtained by a Data Recipient shall apply to all Affiliated Practitioners who are providing health care services to patients (i) at the Participant's facilities; (ii) in their capacity as employees or contractors of the Participant; or (iii) in the course of cross-coverage or on-call arrangements with the Participant or one of the Participant's Practitioners.

   c. An Affirmative Consent authorizing access by an Accountable Care Organization ("ACO"), Independent Practice Association ("IPA"), Physician-Hospital Organization ("PHO"), or similar organization, shall cover only the ACO, IPA, PHO or similar organization itself, and not the health care providers participating in the ACO, IPA, PHO, or similar organization.

   d. The Hixny Patient Consent Form must be used in all instances.

   e. 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.

   f. A patient's consent to a particular Data Recipient allows such Data Recipient to access all patient data uploaded onto the System from any Data Provider that has data concerning such patient, including Sensitive Health Information. Patients cannot limit or "filter" the patient data that will be accessed by the Data Recipient.

   g. In order for consent to be "informed" and "meaningful," any communications with patients regarding consent must be in a language the patient understands or in a manner appropriate for the patient's circumstances if the patient is visually or hearing impaired and in accordance with State and Federal laws, rules and regulations.

   h. Participants may not condition Treatment/coverage on the patient's willingness to consent to the access of their Protected Health Information through the System.

2. Informed Consent. In order to ensure that consent is informed, the Data Recipient must advise the patient of the following:

   a. The Data Recipient's intended use of the patient's health information that is obtained through Hixny, which must be limited to Treatment, Care Management and/or Quality Improvement, and Insurance Coverage Verification.

   b. The other Participants that are participating in Hixny at the time that the patient gives his/her consent by providing the patient with the current Hixny List of Participants in written form or directing the patient to go to the Hixny website, www.hixny.org.

   c. The fact that the Hixny List of Participants may change over time and that the patient may obtain a current listing by going to Hixny's website, www.hixny.org.

d. The Data Recipient will be able to access all of the patient's health information from all other Participants who are Data Providers, if patient consent is received, and that the patient may not limit or "filter" any of the health information that is accessible.

e. The Data Recipient will have access to the following Sensitive Health Information:

i. HIV-related information (New York State Public Health Law, Article 27F);

ii. Mental health information (New York State Mental Hygiene Law §33.13);

iii. Genetic testing information (New York State Civil Rights Law §79-1);

iv. Sexually transmitted disease and reproductive health information, including abortion (New York State Public Health Law §17); and

v. Alcohol and substance abuse Treatment information (42 CFR Part 2).

f. The patient's consent applies to all of Data Recipient's Authorized Users who have a need to know or access the patient's health information, in accordance with applicable laws and regulations and the Hixny Data Exchange Policies and Procedures.

g. The patient's consent applies to Data Recipient's legal affiliates if Data Recipient has entered into a Participation Agreement on such affiliates' behalf.

h. The patient may revoke his/her consent at any time upon written request. However, any health information that Data Recipient accessed from the System prior to the effective date of revocation will remain part of the medical records maintained by the Data Recipient for the patient.

i. The patient may choose to not allow Data Recipient to access his/her health information by refusing to sign the Hixny Patient Consent Form or by denying consent for the Data Recipient on the Hixny Patient Consent Form.

j. Patients shall have the option, through the use of a single paper or electronic form, to affirmatively deny consent for all Hixny Participants to access the patient's information.

k. If patient denies consent, Data Recipient will not have access to the patient's health information even in an emergency situation.

3. Data Recipient's Responsibilities

a. Data Recipient shall ensure that all patient consents obtained are "informed" by following the procedures set forth in Section 2 above and Section 6 below.

b. Data Recipient shall ensure that all patient consents are in writing using the Hixny Patient Consent Form.

c. Data Recipient will provide patients with Hixny and/or NYS educational materials as needed.

d. Once patient consent is received, Data Recipient shall flag such consent in the System. Consent is effective immediately once Data Recipient has flagged such consent in the System. Data Recipient is responsible for maintaining the Hixny Patient Consent Form in the same manner that it maintains other patient consent forms. Upon Hixny's request, Data Recipient shall allow Hixny access to the

Hixny Patient Consent Forms within 5 business days of such request. The Data Recipient shall be responsible for producing all requested consent forms. If unable to meet that criteria a second sampling will be requested. During this process, consent status would be reset to "not asked" or "null" for any patient for whom the Data Recipient could not produce the forms. If the Data Recipient is unable to produce the forms after the second sampling then Hixny, at its sole discretion, will have the right to impose sanctions. Please refer to Hixny's sanction policy, Policy L4800.

e. If a patient wishes to revoke his or her consent, Data Recipient shall

i. have the patient execute the Hixny Withdrawal of Consent Form;

ii. change the patient's consent in the System; and

iii. maintain the original Hixny Withdrawal of Consent Form in the same manner that Data Recipient maintains the Hixny Consent Form.

iv. Revocation is effective immediately once Data Recipient has changed the patient's consent designation in the System.

f. Data Recipient shall not access any patient information from the System unless patient consent is obtained in accordance with this Policy and shall only access it for purposes of Treatment, Quality Improvement, Care Management or Insurance Coverage Verifications, unless otherwise specifically allowed under this policy.

4. Consent by or for Minors

a. A minor's protected health information that is not Minor Consent Information may be accessed based on Affirmative Written Consent (via the Hixny Consent Form) provided by the minor's Personal Representative.

b. If federal or New York law requires the minor's authorization for Minor Consent Information, the Participant may not access such information without the minor's Affirmative Consent and neither Participant nor Hixny may disclose such Minor Consent Information to the minor's Personal Representative without the minor's Affirmative Consent.

c. Parents who share joint custody of a minor have equal authority to provide written consent for such minor and consent by either parent is sufficient.

d. If a court order clearly permits one parent to make health care decisions for a minor, that parent has the authority to provide written consent for such minor. If the court order is not clear as to which parent has the authority to make health care decisions, both parents must provide written consent for a minor.

e. Foster parents or other individuals who have legal custody must provide written documentation to evidence their legal authority to consent before the Participant accepts their written consent to access the health information of a minor.

5. Consent on Behalf of Adult Patients Who Lack Capacity. For adult patients who lack capacity, as determined in accordance with New York law, affirmative written consent must be obtained in accordance with New York law and the Data Recipient's standard policies and procedures governing health care decision-making.

6. Restrictions on Disclosures to Payor Organizations.

a. A Payor Organization may not access, and no disclosures will be made to it of, a patient's PHI where the patient has requested that no disclosures be made.

b. Upon a Data Recipient's receipt of a patient's request that PHI created by a Provider Organization not be disclosed to a Payor Organization, a Data Recipient will have the patient complete a Restriction on Disclosures/Withdrawal of Consent Form, so that any affirmative written consent previously granted to such Payor Organization is revoked. Such revocation remains in effect permanently unless and until the patient submits a new consent form granting the Payor Organization access.

c. An affirmative written consent covering a Payor Organization shall include a notice to the patient that his or her provision of consent will revoke any prior request for a restriction on the disclosure of PHI by any Provider Organization to the Payor Organization and the consent is rejected if the patient indicates she or he does not agree with the revocation of his or her prior request.

d. Provider Organizations and other Data Recipients must clearly inform the patient regarding the following:

i. A patient consenting to a Payor Organization accessing his/her data must be informed that this consent allows the Payor Organization to access all clinical data, including data for Treatments that the patient paid for out-of-pocket without going through a Payor Organization.

ii. A patient choosing to pay out-of-pocket for Treatment at a Participant must be informed that, to prevent a Payor Organization from accessing data from this Treatment, the patient must revoke any Hixny consent previously given allowing that Payor Organization to access data. Such revocation will apply to all of the patient's data and not just data related to the Treatment paid for out-of-pocket.

7. Exceptions to Affirmative Written Consent. In the following limited situations, affirmative written consent is not required:

a. Up-Loading Data by Data Providers. Hixny, acting as a Participant's "business associate" (as defined by HIPAA), holds patient data solely as a custodian for the Participants and does not make data available to other entities without patient consent. Therefore, such storage of data is not treated as a "disclosure" to a third party requiring consent under New York law. Accordingly, Data Providers may upload patient information to Hixny without patient consent.

b. Emergency Situations. A patient's PHI must be made available by Hixny to emergency care providers in order to prevent or lessen the threat to the health and/or safety of the patient. Such access is called "Break the Glass" and is governed by the Break the Glass Policy (*see* Break the Glass Policy herein for terms and conditions for such access).

c. Public Health Reporting.

i. On behalf of a Data Provider, Hixny may make disclosures of PHI to a government agency for purposes of Public Health reporting if the Data Provider is allowed to do so without patient consent under applicable State and Federal laws and regulations. Such purposes include the following:

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

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

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

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

(e) For other Public Health purposes authorized by law.

ii. A patient's denial of consent for all Participants to access the patient's PHI under Section 2 above shall not prevent or otherwise restrict a Public Health Agency from accessing the patient's PHI through Hixny for the purposes set forth in purposes listed above.

iii. Hixny shall track, at the time of access, each access to PHI by Public Health Agency Authorized Users, including the reason(s) for such access.

iv. Hixny shall audit access by Public Health Agency Authorized Users on a regular basis. The audit report shall include the patient names, times, dates, and the reason(s) for each Public Health Agency Authorized User's access of PHI. Hixny, at its sole discretion, will have the right to impose sanctions for any violation of this policy. Please refer to Hixny's Sanction Policy, Policy L 4800.

v. Hixny shall list the name of the Authorized User and Public Health Agency in the patient Audit Logs.

vi. Except for the types of disclosures to Public Health Agencies listed above, no other disclosures of PHI shall be made by Hixny to governmental agencies, including disclosures for health care oversight activities (e.g., Medicaid audits, provider licensing reviews, and fraud and abuse investigations), unless the individuals who are the subjects of such requested PHI have given their affirmative written consent to such disclosure.

d. <u>Disaster Tracking by Disaster Relief Agency</u>

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

(a) Patient name and other demographic information in accordance with the principles set forth in Hixny's access policies and procedures;

(b) Name of the facility or facilities from which the patient received care during the Emergency Event;

(c) Dates of patient admission and/or discharge.

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

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

iv. A patient's denial of consent for all Participants to access the patient's Protected Health Information under Section 2 shall not restrict a Disaster Relief Agency from accessing information as permitted by this section.

e. Improvement and Evaluation of Hixny's Operations. Affirmative patient consent is not required for the following, so long as, consistent with HIPAA, access to PHI will be limited to the minimum amount necessary to accomplish the intended purpose of the use or disclosure:

i. Hixny, government agencies and their contractors to access PHI for the purpose of evaluating and improving Hixny's operations;

ii. Hixny or its contractors to access PHI to enable Hixny to perform system maintenance, testing and troubleshooting and to provide similar operational and technical support; and

iii. Hixny or its contractors to access PHI at the request of a Participant in order to assist the Participant in carrying out activities for which the Participant has obtained the patient's Affirmative Consent. Such access must be consistent with the terms of the Business Associate Agreement entered into by the Participant and Hixny.

f. De-Identified Data.

i. Affirmative Consent is not required for access to De-Identified Data via the System for the following purposes only:

(a) By Hixny, a Participant, or a government agency for research approved by an institutional review board or privacy board organized and operating in accordance with 45 CFR Section 164 in accordance with Section 7(g); or

(b) By a Participant for Quality Improvement, provided that a specially designated committee appointed by Hixny reviews and approves the Quality Improvement activity and Participant makes available to the committee the methodology of the project, which Hixny will make accessible to other Participants and the general public; or

(c) Any purpose for which Hixny, Participant or government agency may access Protected Health Information under these Policies and Procedures; or

(d) By Hixny to perform an evaluation of the economic or other value of Hixny.

ii. Hixny may access Protected Health Information to create and validate the accuracy of De-Identified Data.

iii. Participants shall comply with HIPAA's standards for the de-identification of data, as set forth in 45 CFR Section 164.514, and shall subject any use of De-Identified data to adequate restrictions on the re-identification of such data.

g. Research. Affirmative Consent it not required for Hixny or a Participant to access De-Identified Data or a Limited Data Set in order to conduct Research approved or deemed exempt by an institutional review board organized and operated in accordance with 45 CFR Section 164, subject to the following:

i. Participant shall obtain approval for the Research from Hixny's research committee, which shall apply standards for such reviews, and Participant shall make available to the research committee the methodology of any proposed Research project, which Hixny will make accessible to other Participants and the general public; and

ii. Participant cannot opt out of having its PHI de-identified or converted into a Limited Data Set and used for Research described in this section.

h. One-to-One Exchanges. A Participant may access a patient's PHI via the System from another Participant without Affirmative Consent if such access is considered a One-to-One Exchange and complies with the following:

i. A One-to-One Exchange is an electronic transmission of information that is understood and predictable to a patient because it mirrors a paper-based exchange. One-to-One Exchanges include, but are not limited to, the following: (a) a referral for Treatment or consultation from one health care provider to another; (b) lab or other test results sent to the Practitioner who ordered a diagnostic service; (c) clinical information sent from a Participant to the patient's Payor Organization for Quality Improvement or Care Management/care coordination activities pursuant to an agreement between the Participant and Payor Organization, unless patient has restricted such disclosures in accordance with Section 6; or (d) a discharge summary sent to a discharged patient's primary care provider and/or referring provider.

ii. Participants in a One-to-One Exchange must comply with all Federal and State laws and regulations requiring patient consent for the disclosure and re-disclosure of information by health care providers.[1] The Participant sending information via a One-to-One Exchange message is responsible for ensuring that the content of the message complies with such laws and regulations.

iii. One-to-One Exchange messages can be used to update the Hixny clinical records as well as be forwarded to the Participant that is the intended recipient where applicable. For instance, hospital admissions, diagnostic results, and discharge summaries generally update the Hixny records as well as can be transmitted to an intended recipient identified on the message as a One-to-One Exchange.

iv. Hixny may be required to convert One-to-One Exchange messages in order to match the content form and transmission standard used by the Participant receiving the message. All Participants engaging in One-to-One Exchanges acknowledge and understand that such conversions may result in lost or incomplete data, for which Hixny assumes no responsibility.

[1] New York law currently requires patient consent for the disclosure of information by health care providers for non-emergency treatment purposes. For general medical information, this consent may be explicit or implicit, written or oral, depending on the circumstances. The disclosure of certain types of sensitive health information may require a specific written consent. Under federal law (HIPAA), if the consent is not a HIPAA-compliant authorization, disclosures for health care operations are limited to the minimum necessary information to accomplish the intended purpose of the disclosure. Also, disclosures of information to another Participant for health care operations of the Participant that receives the information are only permitted if each entity either has or had a relationship with the patient, and the information pertains to such relationship.

i. Access to Data Provided by Data Providers. On behalf of a Data Provider, Hixny may allow Authorized Users of the Data Provider to access the data provided to Hixny by that Data Provider for any reason deemed necessary by the Data Provider, including but not limited to Treatment, Quality Improvement or Care Management. Data Providers allowing their Authorized Users to access such data is understood and predictable to a patient because it mirrors access to systems within a Data Provider, such as an electronic health record system, which the same users may have access to without a healthcare information exchange. Such access will not include data from other Data Providers, unless the requirements for patient consent have been obtained in accordance with this policy. Access to a Data Provider's own data is subject to the same logging and auditing requirements that apply to all other data accessed through Hixny, as provided for in Hixny's policies and procedures. Data Providers and Authorized Users are subject to all laws and regulations regarding disclosure of PHI with respect to such data. The foregoing policy and requirements also apply to lab processing results requested by, and fed through Hixny's exchange, from certain lab vendors to Payor Organizations.

References:

42 CFR Part 2
45 CFR Part 164
New York State Civil Rights Law §79-1
New York State Mental Hygiene Law §33.13
New York State Public Health Law §17
New York State Public Health Law §2504
New York State Public Health Law, Article 27-F
New York State Public Health Law, Article 29-C
Standardized Consumer Consent Policies and Procedures for RHIOs in New York State, New York Health Information Security and Privacy Collaboration, December 21, 2007
The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange, ©2006, Markle Foundation
The Statewide Collaboration Process: Privacy and Security Policies and Procedures for RHIOs and their Participants in New York State, Version 2.0, NYeHealth Collaborative
The Statewide Collaboration Process: Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State, Version 3.2, NYeHealth Collaborative (as of June 2015)

Hixny Audit Policy

Policy Number	**L4600**
Policy Description	**This policy describes the responsibilities of both Hixny and its Data Recipients in conducting periodic audits of exchange security and access.**
Policy Intent	**To ensure that the responsibilities of both Hixny and its Data Recipients to monitor and control system access are documented and agreed upon.**
Applies to	**Hixny and its Data Recipients.**
Original Policy Date	**2/25/2009**
Revision History	**10/15/2010; 11/2/2012 (BTG Policy references), 3/13/2015**

Principles

1. Hixny will maintain the Audit Logs generated by the System and will provide its Data Recipients with information from these logs as appropriate.
2. Hixny will take appropriate steps to ensure that appropriate Data Recipient access reviews have been conducted.
3. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Hixny Responsibilities

   a. Hixny will maintain for ten years immutable Audit Logs (logs whose information either cannot be changed or cannot be changed without leaving a record of the change), which contain, at a minimum, the following:
      i. Patient name
      ii. Authorized User Name
      iii. Authorized User's Data Recipient Association
      iv. The type of PHI or record accessed (e.g. pharmacy data, laboratory data, etc.)
      iv. Access Event (Patient Search, Break the Glass, etc.)
      v. Data Providers in Access Event
      vi. Date and Time of Access
      vii. Unsuccessful logon attempts

   b. Hixny requires each Data Recipient to conduct audits of its use of the System, using statistically valid sample sizes. These audits will minimally include:
      i. Annual audits verifying that Affirmative Consent forms are on file for patients whose data is accessed in non-emergency situations;

ii. Annual audits verifying that the Data Recipient's Authorized Users are accessing PHI for authorized purposes only;

v. Audits verifying that the Data Recipient's Authorized Users have met the emergency definition requirements when using the Break–the Glass function (*see* Break the Glass Policy for specific auditing requirements).

vi. Audits verifying Data Recipient's list of active Authorized Users.Audits verifying Data Recipient's Authorized Users meet the Identity Proofing requirements listed in the Hixny Participant Requirement Policy, Section 2.c.

c. Hixny shall review a statistically valid subset of Data Recipient audits for quality and compliance with the requirements above.

d. Hixny shall make the results of these audits available on its web site not later than 30 days after their completion and approval

e. Hixny will provide, within 10 days of the request of any Data Recipient, the following information for a patient of that Data Recipient who has affirmatively consented to that Data Recipient accessing his/her data:

i. The name of each Authorized User who accessed the patient's PHI, covering a period of up to six years immediately prior to the receipt of that request.

ii. The date and time of such access

iii. The types of PHI or record accessed (e.g., clinical data, laboratory data, etc.)

f. Hixny shall support Data Recipients in meeting patient requests for access to Hixny Audit Logs as discussed below under Data Recipient responsibilities.

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

2. <u>Data Recipient Responsibilities</u>

a. Hixny shall, on a regular basis, provide Audit Log containing the data outlined above to Data Recipients, detailing accesses to PHI by that Data Recipient's Authorized Users. Each Data Recipient will review of this information to identify any inappropriate access. Upon the specific request of Hixny, Data Recipient shall confirm to Hixny that such a review has been completed.

b. Upon the request of Hixny, Data Recipients will conduct an audit as described in the Hixny Responsibilities section above.

c. Within 10 days of the receipt of a request from a patient, Data Recipient will provide that patient with the following information, covering a period of up to six years immediately prior to the receipt of that request

i. The name of each Authorized User who accessed the patient's PHI

ii. The Hixny Data Recipient through which this information was accessed

iii. The date and time of such access

iv. The types of PHI or record accessed (e.g., clinical data, laboratory data, etc.)

d. Data Recipient must process one patient data request per twelve-month period at no cost to the patient. For multiple patient data requests within that period, Data Recipient may, with the agreement of Hixny, charge the patient a reasonable fee. However, this fee shall be waived if it is determined that the patient had reasonable cause to suspect the confidentiality of his/her data had been Breached.

e. Data Recipient must post a notice describing the availability of Hixny information on its web site.

f. Data Recipient shall be required to maintain all required documents and records for seven years.

g. Participants shall provide access to information required by Hixny to fulfill its reporting, auditing, and investigative obligations under its Qualified Entity Participation Agreement with NYeC.

h. In the event of an audit by a government regulatory agency or any other entity authorized to conduct an audit of behalf of a government regulatory agency, Participants shall provide access to SHIN-NY-related information by such regulatory agency (or its authorized agent) or Hixny.

i. If a Data Recipient accesses PHI through a Certified Application, the audits described in this Policy shall include access by the Data Recipient's users through the Data Recipient's system.

3. Sanctions

a. Hixny, at its sole discretion, will have the right to impose sanctions for any violation of this policy. Please refer to Hixny's Sanction Policy, Policy L4800.

Hixny Sanction Policy

Policy Number	**L4800**
Policy Description	**This policy describes the responsibilities of both Hixny and its Participants in situations in which sanctions must be enforced against the Participant or Authorized User**
Policy Intent	**To ensure that Participants are enforcing policies and procedures listed within this document**
Applies to	**Hixny and its Participants**
Original Policy Date	**6/2014**
Revision History	**None**

Principles

1. Sanctions are an important mechanism for ensuring that Participants and Authorized Users comply with the policies and procedures as outlined within the Data Exchange Policies and Procedures. Hixny shall apply, or require Participants to apply sanctions in the event of policy violations. The provisions in this policy are designed to provide guidelines for the imposition of sanctions, while leaving flexibility to determine appropriate sanctions on a case by case basis.
2. Hixny may modify this policy from time to time with Board approval.

Procedures

1. When determining the type of sanctions to apply, Hixny and/or its 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/or
   d. Whether the violation resulted in harm to a patient or other person.
2. Sanctions shall include, but do not necessarily have to be limited to:
   a. Temporarily restricting an Authorized User's access to Hixny;
   b. Terminating an Authorized User's access to Hixny;
   c. Suspending or terminating a Participant's participation in Hixny; and/or
   d. The assessment of fines or other monetary penalties.
3. Hixny, at its sole discretion, will have the right to impose sanctions for any violations of the Data Exchange Policies and Procedures.

Hixny Breach Policy

Policy Number	**L4500**
Policy Description	**This policy describes the responsibilities of both Hixny and its Participants in situations in which a Breach of Unsecured PHI via the System has occurred.**
Policy Intent	**To ensure that violators are held accountable, assure patients about Hixny's commitment to privacy, and mitigate any harm that privacy violations may cause.**
Applies to	**Hixny and its Participants**
Original Policy Date	**10/15/2010**
Revision History	**3/15/2015, ____/2016**

Principles

1. Hixny and its Participants will investigate and mitigate, to the highest degree possible, any unauthorized access or release of Unsecured PHI or access or use of the System.
2. Hixny will require affected Participants to participate in the reporting, investigation and mitigation of any actual or suspected Breach that affects their data.
3. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Participant Responsibilities

   a. Each Participant shall have a mechanism for, and shall require, all Authorized Users and other workforce members, agents, and contractors to report any actual or suspected Breach of Unsecured PHI accessed via the System. Each Participant also shall establish a process for individuals whose PHI is included in the System to report any real or suspected Breach of Unsecured PHI.

   b. A Participant that becomes aware of a report of an actual or suspected Breach of Unsecured PHI from any source must report this possible Breach to Hixny in writing. This report must be made as soon as practical but no later than ten (10) calendar days of Participant having knowledge of the possible Breach. Such notice shall (i) identify the nature of the Breach; (ii) identify the date of the Breach and the date of the discovery of such event, if known; (iii) identify the PHI used or disclosed and the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Participant to have been, accessed, acquired, used, or disclosed during the Breach; (iv) identify who made the non-permitted use or received the non-permitted disclosure; (v) identify what corrective action the Participant took or will take to prevent future similar Reportable Events; (vi) identify what the Participant did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and (vii) provide such other information, including a written report, as Hixny may reasonably request.

c. Each affected Participant will cooperate fully with Hixny in all identification, mitigation, correction and notification activities that result from the identification of a Breach.

2. Hixny Responsibilities

a. Hixny shall report to a Participant any Breach of a Participant's Unsecured PHI accessed via the System that Hixny becomes aware of, either through notification by a Participant or otherwise. Such notice shall be made in accordance with the timeframes and notification requirements set forth in the Business Associate Agreement between Hixny and the Participant, even if not caused by Hixny.

b. The Hixny CEO, or his/her designee, will lead to the investigation of all real and suspected Breaches that Hixny becomes aware of, either from a Participant's report or otherwise. Such investigation will include at least one Hixny staff member and at least one representative from the Participant reporting the Breach, if any. The following steps will be taken:

i. Investigation of (or requiring the applicable Participant to investigate) the severity (scope and magnitude) of the suspected Breach;

ii. Determination of whether an actual Breach via the System has occurred in accordance with HIPAA.
iii. Identification of the root cause of the Breach.

c. If it is determined that an actual Breach has occurred, Hixny will:

i. Notify any impacted Participants that their data is affected by the Breach in accordance with Section 2(a);

ii. Mitigate (or require the applicable Participant to mitigate), to the extent practicable, any harmful effects of such Breach that is known to Hixny or the Participant, where the level of mitigation activity shall be consistent with the severity of the Breach and whether the Breach was caused by Hixny or a Participant;

iii. Notify any other impacted Participants of the mitigation efforts and corrective actions being taken as a result of the Breach; and

iv. Coordinate the issuance of (or require the applicable Participant to issue) any notifications to affected patients and legal/regulatory agencies that are required by federal and state laws and regulations, if requested by the affected Participant and agreed to by Hixny.

v. Execute the Hixny Crisis Communication Plan to ensure appropriate communication with entities outside Hixny (media, etc.) is initiated and maintained, if required and/or appropriate given the circumstances.

f. Hixny shall document all actions taken, including but not limited to:

i. Investigations and interviews conducted;

ii. Determination as to whether a Breach has occurred, including Hixny's assessment of applicable risk factors and its determination about the probability that PHI has been compromised;

iii. Any mitigation efforts or corrective actions taken; and

iv. Any notifications made.

3. Sanctions

a. Hixny, at its sole discretion, will have the right to impose sanctions for any violation of this policy. Please refer to Hixny's sanction policy, Policy L4800.

References:

45 CFR 164 Subpart D.
HIPAA Final Rule, 78 Fed. Reg. 5565 (Jan. 25, 2013).
The Statewide Collaboration Process: Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State, Version 3.2, NYeHealth Collaborative (as of June 2015).
Hixny Standard Business Associate Agreement (as of March 2016).

Hixny Break the Glass Policy

Policy Number	**L4700**
Policy Description	**This policy describes when a treating Practitioner who is an Authorized User may access a patient's PHI in an emergency situation without the patient's affirmative written consent, Hixny's right to audit and track such access, and sanctions for breaking the glass in violation of this policy.**
Policy Intent	**To ensure that Break the Glass access complies with NYS Privacy and Security Policies and Procedures, Section 1.2.3.**
Applies to	**All Participants, Data Recipients, Authorized Users, Practitioners and Hixny staff.**
Original Policy Date	**11/2/2012**
Revision History	**3/13/2015**

Principles

1. Data Recipients and their Authorized Users may not access PHI from the System unless the patient has provided affirmative written consent, unless an exception applies.
2. The NYS Privacy and Security Policies and Procedures, Section 1.2.4, provides that a treating Practitioner who is an Authorized User, an Authorized User acting under the direction of a treating Practitioner, or an Advanced Emergency Medical Technician may "Break the Glass" – i.e., access PHI via the System without obtaining affirmative written consent – if the Practitioner or the Advanced Emergency Medical Technician determines, in his/her reasonable judgment, that an emergency situation exists.
3. For purposes of this policy, "emergency situation" means the following: In the Practitioner's or Advance Emergency Medical Technician's reasonable 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.
4. For purposes of this policy, "Practitioner" refers to a treating Practitioner who is an Authorized User.
5. Hixny may modify this policy from time to time with the approval of the Board of Directors.

Procedures

1. <u>Conditions for Breaking the Glass</u>

   a. An Authorized User who is a treating Practitioner or who is acting under the direction of a treating Practitioner, or an Advanced Emergency Medical Technician may access a patient's PHI in an emergency situation if the following conditions are met:

i. In the Practitioner's or Advanced Emergency Medical Technician's reasonable judgment, an emergency situation 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 treating Practitioner or Advanced Emergency Medical Technician determines in his/her reasonable judgment that the System may hold information that may be material for the Treatment of the patient;

iii. The patient has not denied consent for the Data Recipient to access his/her information;

iv. In the event than an Authorized User acting under the direction of a treating Practitioner Breaks the Glass, such Authorized User must record the name of the Practitioner providing such direction; and

v. The treating Practitioner, Authorized User acting under the direction of a treating Practitioner, or Advanced Emergency Medical Technician attests in the System that foregoing conditions have been met before accessing any of the patient's health information.

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. A Practitioner's right to access the System in a "Break the Glass" situation terminates upon the completion of the emergency Treatment. The Data Recipient shall ensure that access by the treating Practitioner terminates upon the completion of the emergency Treatment.

d. Only those Authorized Users assigned the "Break the Glass" role by Hixny in accordance with Hixny's Services Policy, L4300, may access the System in a "Break the Glass" situation.

e. Where a patient has previously withheld or revoked/withdrawn consent for a particular Data Recipient or all Data Recipients, the patient's health information may not be accessed even in an emergency situation.

f. Notwithstanding anything to the contrary set forth in Hixny's policies, a Data Recipient is not responsible for specifically excluding any Sensitive Health Information from access through the System in a "Break the Glass" situation.

2. Auditing, Tracking and Categorizing Break the Glass ("BTG") Access

a. Hixny shall audit and track all BTG events and provide Data Recipients with a list of BTG events within their facility on at least a monthly basis.

b. Hixny shall promptly notify their Data Suppliers that are federally-assisted alcohol or drug abuse programs when Protected Health Information from the Data Supplier's records is accessed. 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.

c. Upon a patients' 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 lieu of providing such notice, Participants that are hospitals may notify all patients discharged from an emergency room that their PHI may have been accessed during a Break the Glass incident and inform patients how they may request an Audit Log to

determine if such access occurred. The notice required by this Section shall be provided within ten days of the patient's discharge.

d. Data Recipients must provide Hixny with a detailed report related to all BTG events within ten (10) business days after notification of the event, including the following information: (i) date of access, (ii) name of patient accessed, (iii) MRN of patient accessed, (iv) verification that an Authorized User who was the treating Practitioner broke the glass, (v) verification that the requirements for BTG access were met, (vi) confirmation that the patient was informed that the Practitioner accessed his/her PHI, and (vii) such additional information as determined by Hixny.

e. If a Data Recipient has obtained a patient's affirmative written consent but the Hixny HIE has not yet recorded such consent, access by the treating Practitioner will not be considered a BTG access for further review.

f. Hixny will review all reports and categorize each incident as one of the following:

   i. Appropriate BTG Access, which means the conditions set forth in Section 1 were met; or

   ii. Accidental Access, which means the conditions for BTG access did not exist but the Practitioner broke the glass in good faith because he/she (A) mistakenly believed that affirmative written consent had been collected, or (B) did not understand the requirements for BTG access.

   iii. Inappropriate Access, which means any other instances where the glass was broken but the requirements for BTG access were not met, as determined by Hixny in its sole discretion. Inappropriate Access includes, but is not limited to, the following: (A) instances where the Practitioner believes that medical history is necessary for the Treatment of the patient but it is not an emergency, (B) breaking the glass by an Authorized User who is not the treating Practitioner, or (C) a Breach of Unsecured PHI in violation of HIPAA or NYS law, as defined in Hixny's Breach Policy.

3. Sanctions

a. Hixny, at its sole discretion, will have the right to impose sanctions for any violation of this policy. Please refer to Hixny's Sanction Policy, Policy L4800.

Hixny Patient Portal – Registration and Authorization Process

Policy Number	**L4800**
Policy Description	**This policy describes the registration and authorization process for Patients using of the Patient Portal.**
Policy Intent	**To ensure that Patients agree to the terms and conditions associated with usage of the Patient Portal and Patients' identities are properly verified before gaining access to Patient Data via the Patient Portal.**
Applies to	**All Patients accessing Patient Data via the Patient Portal and Hixny and all Participants that are performing the registration/authorizing process.**
Original Policy Date	
Revision History	**11/8/2013**

Principles

1. Hixny has established a process for registering and authorizing Patients to use the Patient Portal to access Patient Data.
2. Hixny has established a process for verifying that a Patient is who he or she claims to be, before such Patient is authorized to access Patient Data through the Patient Portal.
3. If not defined herein, capitalized terms are defined in the Definitions section of the Hixny Data Exchange Policies and Procedures.
4. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Registration and Authorization

    a. Registration Required. Only Patients who are registered with Hixny and execute a Patient Portal Participation Agreement are permitted to use the Patient Portal to access the Patient's Patient Data.

    b. Registration Authority. Hixny shall have registration authority and certain Participants shall have authority to assist Hixny in the registration process if approved by Hixny. If so approved, such Participants are subject to this policy.

c. Registration Process.

i. Participants with registration authority shall assist Patients wishing to register by accessing the Registration Application available in electronic form on Hixny's website (www.hixny.org) and helping Patients to complete the initial part of the Registration Application.

ii. In order to be authorized to access the Patient Portal, Patients are required to submit all information requested by Hixny.

iii. Hixny will provide Participants with educational materials/information to provide to and/or explain to Patients during the registration process. Participants are required to provide such education to Patients.

iv. For any Patient a Participant assists with completing the Registration Application, such Participant shall verify the identity of the Patient by following Participant's standard policies and procedures for verifying the identity of patients upon admission/registration. Participant agrees to use the same level of diligence Participant typically uses to verify a patient's identity. If Participant is unable to verify the identity of a Patient, Participant shall instruct Patient to contact Hixny directly and inform Hixny of the same.

v. As part of the application process, Participant shall also determine whether Patient is capable of giving informed consent by applying Participant's standard policies and procedures. If Participant determines that Patient is unable to give informed consent, Participant shall instruct Patient to contact Hixny directly and inform Hixny of the same.

vi. Hixny reserves the right to ask for additional information as needed to complete the registration and authorization process at the time of registration or at any other time Hixny deems necessary in order to verify the Patient's identity.

vii. After the first part of the Registration Application is completed, Hixny will send a confirming email to the Patient. Such email will include the Patient Portal Participation Agreement, which specifies the terms and conditions of the Patient's use of the Patient Portal. A Patient must electronically sign the Patient Portal Participation Agreement in order for the Registration Application to be complete.

d. Approval of Registration Applications. Hixny shall confirm the Patient Portal Participation Agreement is executed and approve or disapprove the Registration Application, in its sole discretion, within a reasonable time after submission, as determined by Hixny.

e. Notice of Authorization to Use Patient Portal. Hixny shall provide to Patient an electronic notice of approval or disapproval of registration. If Patient's Registration Application is approved, Patient will be authorized to use the Patient Portal ("Patient Portal User").

Hixny Patient Portal – Access Policy for Participant-Contributed Patient Data

Policy Number	**L4900**
Policy Description	**This policy describes what Patient Data will be accessible by Patients via the Patient Portal, which Patients may be granted access, and when access may be denied.**
Policy Intent	**To ensure Patient Portal Users understand what information is available via the Patient Portal and why access may be denied.**
Applies to	**All Patient Portal Users accessing Patient Data via the Patient Portal and any Participants seeking to deny access.**
Original Policy Date	
Revision History	**7/13/2015**

Principles

1. Patients have the right to access their medical records under New York State law and the Health Information Protection and Accountability Act ("HIPAA") and its implementing regulations, as amended, and other Federal and State statutory or regulatory requirements (collectively, "Federal and State Requirements"), subject to certain limitations.
2. Notwithstanding the foregoing, Federal and State Requirements give Participants the right to deny access in certain circumstances, including but not limited to situations where a licensed health care professional, in the exercise of professional judgment, believes that the access requested is reasonably likely to endanger the life or physical safety of the Patient.
3. If not defined herein, capitalized terms are defined in the Definitions section of the Hixny Data Exchange Policies and Procedures.
4. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Patients Who May Be Authorized To Access Patient Data

   a. As of the date of this policy, adults with the ability to give informed consent for health care decision making for themselves.

   b. At such time as determined by Hixny, individuals with legal authority to consent to health care decisions on behalf of a Patient who lacks decision-making capacity, including Health Care Agents appointed via a valid health care proxy, surrogates appointed in accordance with the Family Health Care Decisions Act, Article 81 guardians, parents or legal guardians of children ages 0-9 years, and HIPAA authorizations.

   For purposes of this policy, the foregoing are "Patient Portal Users."

2. Patient Data Available Via Patient Portal

a. As of the date of this policy, Patient Portal Users at a minimum will have access to the following Patient Data that is contributed to the HIE, unless access is denied in accordance with Section II below:

Patient Data from inpatient settings:

- Patient name
- Admit and discharge date and location
- Reason for hospitalization
- Care team including the attending of record as well as other providers of care
- Procedures performed during admission
- Current and past problem list
- Current medication list and medication history
- Current medication allergy list and medication allergy history
- Vital signs at discharge
- Laboratory test results (if made available at time of discharge)
- Summary of care record for transitions of care or referrals to another provider
- Care plan field(s), including goals and instructions
- Discharge instructions for patient
- Demographics maintained by hospital (sex, race, ethnicity, date of birth, preferred language)
- Smoking status

Patient Data from outpatient settings:

- Patient name
- Provider's name and office contact information
- Current and past problem list
- Procedures
- Laboratory test results (subject to Section II.D)
- Current medication list and medication history
- Current medication allergy list and medication allergy history
- Vital signs (height, weight, blood pressure, BMI, growth charts)
- Smoking status
- Demographic information (preferred language, sex, race, ethnicity, date of birth)
- Care plan field(s), including goals and instructions, and any known care team members including the primary care provider (PCP) of record
- Date of service/encounter

c. Patients will not able to access the following Patient Data through the HIE:

a. Lab results performed by commercial lab for outside providers

d. Data Providers providing additional information beyond the minimum values described in Section II(a) shall have the right to display additional information at their discretion, so long as this information meets State and Federal requirements. This may include narrative reports, pathology, imaging radiology reports, and other transcribed documents. Hixny will make this additional information available upon the request of the Data Provider. Nevertheless, Hixny may

not be able to filter the additional content if filtering is requested by the Data Provider. All Data Providers hereby accept such limitation.

e. Special Rule: Hixny will block Patient access to laboratory results from physician practices for two (2) weeks from the date the laboratory results are electronically delivered to the physician practices in order to provide adequate time for review and release to Patient by the Practitioner. Upon the expiration of the two week period, such laboratory results with be accessible to Patient unless Participant blocks Patient's access. Notwithstanding the foregoing, Hixny may grant a shorter delay at the request of the Data Provider.

3. Denial of Access. If a Patient Portal User requests access to Patient Data via the Patient Portal, access may be denied under the following circumstances:

a. Inability to Authenticate Identity. Hixny may deny access if it determines, in its sole discretion, that the identity of the individual seeking access cannot be appropriately authenticated.

b. Participant Requests Denial of Access.

i. In accordance with Federal and State Requirements, a Participant may block a Patient Portal User's access to all Patient Data contributed to the HIE by Participant.

ii. If Participant seeks to block a Patient's access, Hixny will use commercially reasonable efforts to block Patient access to all Patient Data contributed by such Participant to the extent reasonably possible within a reasonable amount of time, as determined by Hixny.

iii. Participant is solely responsible for complying with all Federal and State Requirements regarding the denial of access, including but not limited to determining whether denial of access is legally appropriate, timely notification to the Patient of the denial of access, the reasons for such denial, and the Patient's right to request a review of such denial;

iv. Hixny shall have no responsibility for determining whether the denial of access is appropriate under Federal and State Requirements; and

v. Hixny shall have no liability to Participant or a Patient for blocking a Patient's access to Patient Data, if Hixny acts in good faith to implement a Participant's request to deny such Patient access to Patient Data contributed by Participant through the Patient Portal and if Hixny has not acted in gross negligence or willful misconduct in implementing such request.

Hixny Patient Portal – Access and Use Policy for Patient-Contributed Data

Policy Number	**L5000**
Policy Description	**This policy describes how Patient Data contributed by Patient Portal Users may be used by Hixny and Participants that are Data Recipients.**
Policy Intent	**To ensure Patient Portal Users understand how Patient Data may be used by others.**
Applies to	**All Patient Portal Users who contribute Patient Data via the Patient Portal and any Participants seeking to use such Patient Data.**
Original Policy Date	
Revision History	**7/13/2015**

Principles

1. A Patient Portal User will have the ability to contribute his or her Patient Data to the HIE through the Patient Portal ("Patient-Contributed Data").
2. Similar to Patient Data contributed by Data Providers, Patient-Contributed Data cannot be accessed through the HIE unless the Patient Portal User has given affirmative written consent to a particular Data Recipient by executing the Hixny Patient Consent Form.
3. Notwithstanding Principle #2, Patient-Contributed Data can be disclosed without the Patient Portal User's consent in certain limited situations, which are similar to the situations that apply to Patient Data contributed by Data Providers.
4. If not defined herein, capitalized terms are defined in the Definitions section of the Hixny Data Exchange Policies and Procedures.
5. Hixny may modify this policy from time to time with Board approval.

Procedures

1. Access to Patient-Contributed Data by Patient Portal User. A Patient Portal User may access any Patient Data contributed by such Patient to the HIE via the Patient Portal, subject to Hixny Data Exchange Policies and Procedures regarding logging and auditing requirements.

2. Access to Patient-Contributed Data by Participants/Data Recipients. Access to Patient Data contributed by a Patient Portal User is subject to the same rules that apply to Patient Data contributed by Data Providers, as set forth in the Hixny Patient Consent Policy. More specifically:

    a. Unless an exception described in Section IV applies, a Participant that is a Data Recipient must first obtain Patient Portal User's written consent before the Data Recipient or its Authorized Users may access the Patient Portal User's Patient Data, whether contributed by the Patient Portal User or contributed by other Data Providers.

b. Patient consent for any Patient Data on the HIE is effectuated through the use of the Hixny Patient Consent Form. If a Patient Portal User provided consent to a particular Data Recipient prior to executing a Patient Portal Participation Agreement, such consent shall apply to any Patient Data subsequently contributed by Patient Portal User and new patient consent is not required.

c. A Patient Portal User's consent to a particular Data Recipient allows such Data Recipient to access all Patient Data contributed by Patient Portal User and other Data Providers and uploaded onto the HIE, including Sensitive Health Information. Patient Portal Users cannot limit or "filter" the Patient Data that will be accessed by the Data Recipient.

d. The Data Recipient will have access to the following Sensitive Health Information if contributed to the HIE by Patient Portal User or other Data Providers:

i. HIV-related information (New York State Public Health Law, Article 27F);

ii. Mental health information (New York State Mental Hygiene Law §33.13);

iii. Genetic testing information (New York State Civil Rights Law §79-1);

iv. Sexually transmitted disease and reproductive health information, including abortion (New York State Public Health Law §17); and

v. Alcohol and substance abuse Treatment information (42 CFR Part 2).

e. A Patient Portal User's consent applies to all of Data Recipient's Authorized Users who have a need to know or access such Patient Data, in accordance with applicable laws and regulations and the Hixny Data Exchange Policies and Procedures.

f. A Patient Portal User's consent applies to Data Recipient's legal affiliates if Data Recipient has entered into a Participation Agreement on such affiliates' behalf.

g. A Patient Portal User may revoke his/her consent at any time upon written request. However, any Patient Data that Data Recipient accessed from the HIE prior to the effective date of the revocation, whether contributed by Patient Portal User or other Data Recipients, will remain part of the medical records maintained by the Data Recipient.

3. Use of Patient-Contributed Data by Participants/Data Recipients. Data Recipients may access and use Patient-Contributed Data only for the purposes of Treatment, Quality Improvement and Care Management, in accordance with the Hixny Participation Agreement, the Hixny Data Exchange Policies and Procedures, and applicable Federal and State laws and regulations.

4. Use/Access to Patient-Contributed Data Without Consent. Patient Data contributed by a Patient Portal User is subject to the rules that apply to access and use of Patient Data without affirmative written consent, as set forth in the Hixny Patient Consent Policy. Accordingly, the Patient Portal User's affirmative written consent is NOT required in the following limited situations:

a. Emergency Situations. Hixny has the right to make Patient Portal User's Patient Data available to emergency care providers in order to prevent or lessen the threat to the health and/or safety of the Patient Portal User. Such access is called "Break the Glass" and is governed by the Break the Glass Policy (*see* Break the Glass Policy herein for terms and conditions for such access).

b. Other Situations. Patient Data contributed by a Patient Portal User can be accessed and used without the Patient Portal's affirmative written consent in the following situations, as further described in Hixny's Patient Consent Policy:

i. Public Health reporting
ii. Disaster tracking by Disaster Relief Agency
iii. Improvement and evaluation of Hixny's operations
iv. De-identified data
v. Research
vi. One-to-One Exchanges