Dear Participant,

Welcome to Healthix, the largest regional health information organization (RHIO) in New York State. Before you can gain access to patient data from over 500 facilities and across regions, we will need to review the regulatory requirements that apply to all Healthix participants. To make it all as fast and easy as possible, we have created this Healthix Compliance Plan to organize and communicate those requirements to you.

The Healthix Compliance Plan is divided into sections that have numbered compliance requirements and associated explanations. Some have a process for you to follow, which you may already be doing – in which case this document will serve to validate your efforts. For others, this document will help you understand the requirements and assist in putting a process in place. Other sections will require you to indicate a point of contact at your organization, and finally some sections are purely to provide you with information and validate that you understand it and will comply with New York State Dept. of Health and Healthix Privacy and Security Policies. Please make sure to complete the action steps outlined in each section.

Your Healthix Compliance Coordinator is your main contact for all things related to compliance with Healthix Privacy and Security Policies. He or she is always available to answer your questions and provide continued support to your organization. I look forward to working together and continuing to better our health care system.

Sincerely,
Salvatrice Scerbo
Senior Director of Compliance

Compliance Plan Sections

Section 1: Consent Management

The Healthix consent form will allow the patient to choose a consent option for **Community-Wide Consent** or **Single Participant consent.** Healthix provides its Participants with a standardized 3 option consent form: (1) Give Consent,(2) Deny Consent unless it is to provide the patient with health care services in a medical emergency only or (3) Deny Consent to access any electric health information through Healthix for any purpose even in a medical emergency.

If you wish to customize the form Healthix must approve any alterations before you begin using it.

Each of the following sections explains a requirement your organization must meet in order to be a Healthix participant.

1.1 Implement Statewide Consent Form: Healthix participants need to (1) use a new consent form recently required by NYSDOH and attached as ***Exhibit 1***, or (2) get Healthix approval to use a customized form. However, all consent forms must contain certain statements (*see appendix*):

1.2 Healthix Participant List: The participant will provide the patient with an updated list of Healthix Participants available to Participants. **This list needs to be completed with consent option for Community- Wide Consent.**

1.3 One to One Exchange: A One-to-One Exchange is an electronic transfer of information that mirrors a paper-based exchange such as a referral to a specialist, a discharge summary sent to where the patient is transferred, lab results sent to the Practitioner who ordered them or clinical information sent from a hospital to the patient's health plan for Quality Improvement or Care Management/coordination activities for such patient. A One to One Exchange means a disclosure of Protected Health Information from one Participant to another Participant for the purpose of treatment, quality improvement and/or care management.
***Participants will be expected to complete the required One To One Exchange authorization.

1.4 Break the Glass Access: Sometimes Healthix allows one-time only access to a patient's protected health information *without* his or her affirmative consent. This is called breaking the glass, or BTG. The following criteria has to be met and personally attested to by the individual who is breaking the glass:

- An emergency condition exists if, in the individual's judgement:
  - Patient is in need of immediate medical treatment
  - An attempt to secure consent would result in a delay of treatment, and
  - A delay would increase the risk to the patient's life or health

1.5 Retain Consent Forms for Audit: Retain copies of all completed patient consent forms. You may do so electronically or by hard copy, we just suggest that you be consistent. Healthix will need those saved copies when performing our annual consent audit.

1.6 Withdrawal of Consent: Implement the following procedure: If a patient wishes to revoke or withdraw an affirmative consent (i.e. change from "Give Consent" or "Deny Consent" to "Null/Undecided"), you must verify the patient's identity, document the request, and notify Healthix immediately by contacting your Healthix Account Manager.

1.7 Minors: For minor patients between the ages of birth and 18 years old a parent or guardian may provide consent on behalf of the minor. A clinician providing minor consent services including reproduction, HIV/Aids, sexually transmitted infections, and mental health may ask for additional consent from the minor during the course of treatment.

1.8 Consent Training: Train all staff that collect patient consent on Healthix consent policies and identify a point of contact (POC) responsible for working with Healthix to schedule, conduct, and document all trainings. All such staff must be trained when first hired or when they first start to collect consent, and retrained annually thereafter. Healthix offers "train the trainer" sessions and your Compliance Manager can work with you to structure customized training materials so that you can then conduct your own trainings. If utilizing a train the

trainer model, participants need to send attestation sheets, attached as ***Exhibit 2***, listing names of the staff who are trained and the dates of training to your Compliance Manager as soon as the trainings are completed.

ACTION ITEMS *(date and initial that participant will be in full compliance before Healthix integration project is completed)*

1	Implement Statewide Consent Form	Date	Initials
2	Implement Withdrawal of Consent Procedure	Date	Initials
3	Create & Implement procedure for retaining consent forms	Date	Initials
4	Train all staff that collect patient consent	Date	Initials
5	Identify Contact for Consent Management:		

Full Name	Title	Phone #	email

Section 2: Authentication, Authorization, and Access

2.1 User Acceptance Testing: Designate an individual to perform user acceptance testing. After connectivity has been established between your organization and Healthix, this person will need to approve the form and content of the messages being exchanged to finalize the work.

2.2 Identity Proofing: Verify the identity of each individual whom your organization sponsors and/or validates as an authorized user of Healthix with a valid government issued photo ID, such as a driver's license or passport, and designate an individual that Healthix can contact in the event it needs assistance in confirming the identity of an Authorized User.

2.3 Change of User Role or Employment Status: Notify Healthix when an Authorized User has been terminated from your employment within one business day of termination so that Healthix can disable the individual's access. Some participants may remove the Authorized User via their Active Directory to disable that individual's access to Healthix.

2.4 Role Based Access: Identify an individual that will be responsible for working with Healthix to assign each authorized user a role type. ***Exhibit 3*** contains a table of Healthix user roles.

2.5 **Passwords: Ensure that Authorized Users are assigned a unique user name and that Healthix user passwords shall have a minimum length of 8 characters and contain: upper case letters, lower case letters, and at least one numbers and/or keyboard symbols.

2.6 **Password Change: Authorized User passwords need to change every 90 days.

2.7 **Inactivity of Healthix System: The period of time that the user can keep a session open without entering keystrokes or mouse clicks should not exceed 15 minutes duration, at which point the application must force log-off.

2.8 **Failed Access Attempts: Require a lock-out and password reset after a 5th failed access attempt.

**Note: These requirements apply ONLY if access to Healthix at your organization occurs through your own EHR or

other application (and therefore you set these parameters) -- referred to as “Single Sign On”.

ACTION ITEMS *(date and initial that participant will be in full compliance before Healthix integration project is completed)*

1	Identify Contact for User Acceptance Testing				
Full Name		Title	Phone #	email	
2	Identify Contact for Identity Proofing				
Full Name		Title	Phone #	email	
3	Identify Contact for Provisioning Users				
Full Name		Title	Phone #	email	
4	**Confirm adherence to the Single Sign On requirements			Date	Initials

Section 3: Patient Engagement

This section will ensure you are prepared to address issues that patients may raise about Healthix and to respond to patient requests. The goal is for your organization to be able to help patients understand what information exists about them, how that information is used, and how they can access it.

3.1 Patient Notice: A patient notice needs to be displayed in common areas such as a waiting room. It informs patients that their PHI is being uploaded into Healthix and explains how they may choose to deny consent for all Healthix Participants. Healthix has a standard patient notice you are encouraged to use (***Exhibit 4***), or alternatively we will work with you to approve a customized notice.

3.2 Participant List: Provide the patient with the most updated Healthix Participant List when **with consent option for Community- Wide Consent**

3.3 Access to a Patient’s own PHI: Notify Healthix promptly if a patient asks for access to his or her information in Healthix. The participant will then work with Healthix to obtain such information.

3.4 Corrections: Notify Healthix immediately if, in response to a request by a patient, you or the data supplier make any corrections to erroneous patient information.

3.5 Restrictions on payers: Notify Healthix immediately if a patient, who is paying for his/her health services out of pocket, does not want PHI related to those services disclosed to Healthix or any other organization (typically an insurer).

3.6 Notify Emergency Department patients of a BTG occurrence: If a BTG incident occurred during an emergency room visit, you are required to notify the patient of such incident and inform them how they may request an audit log of the information that was accessed. This requirement may be satisfied by providing notice, within 10 days, to all patients who are discharged from your emergency department. You may use Healthix’s standard BTG signage (***Exhibit 5***) or you may request approval of a customized one.

ACTION ITEMS *(date and initial that participant will be in full compliance before Healthix integration project is completed)*

1	Display Healthix Patient Notice	Date	Initials
2	Provide the patient with the current Healthix Participant List	Date	Initials
3	Notify Healthix Support (support@healthix.org) of items 3.2, 3.3 and 3.4	Date	Initials
4	Display BTG Signage	Date	Initials

Section 4: Sensitive Data *(if applicable)*

1	Do you have any SAMHSA/OASAS funded programs	Yes	No

4.1 Identify SAMHSA/OASAS data providing facilities: Determine whether a federally assisted alcohol or drug treatment program, as defined in 42 CFR Part 2.11, is part of your organization and determine if you contribute data to Healthix from that program. Please refer to ***Exhibit 6*** for the definition of a 42 CFR Part 2 program.

4.2 Qualified Service Organization Agreement (QSOA): If (1) your organization is a federally assisted drug or alcohol abuse program, *or* you have identified such a program that is part of your organization, (2) you receive data from such a program, and (3) you may transmit that data to Healthix, federal law requires that you sign a QSOA. A QSOA is a mechanism that allows for the disclosure of information between a 42 CFR Part 2 Program and an organization that provides services to the program, like Healthix. Once a QSOA is in place, federal law permits the Part 2 program to freely communicate information from patients' records to Healthix, without patient consent, as long as it is limited to that information needed by Healthix to provide services to the program.

4.3 BTG Access of SAMHSA/OASAS data: If you are a 42 CFR Part 2 program, Healthix needs you to identify a point of contact at your organization that will be responsible for receiving a weekly BTG report. This report will serve to notify you of all instances where your organization's data was accessed through Healthix in a BTG situation.

ACTION ITEMS *(date and initial that participant will be in full compliance before Healthix integration project is completed)*

1	Work with Healthix to identify any 42 CFR Part 2 programs	Date	Initials

Section 5: Certified Applications *(if applicable)*

5.1 Work with Healthix to establish your application as a Certified Application. A Certified Application is a computer application certified by Healthix that is used by a Participant to access PHI from Healthix on an automated, system to system basis. This means access to Healthix data bypasses the Healthix system and consequently all of its corresponding privacy and security controls, so we need to verify that your system meets certain minimum security requirements (*see* ***Exhibit 7)***.

ACTION ITEMS *(date and initial that participant will be in full compliance before Healthix integration project is completed)*

		Date	Initials
1	Work with Healthix to establish your application as a Certified Application		

Section 6: Audits

New York State requires Healthix to perform certain periodic audits. As a new Participant, Healthix will conduct an initial audit approximately 6 months after you go live with Healthix services. We will then review the results and establish your annual audit schedule. So, to summarize:

- Initial mini audit approximately 6 months after go live date
- Audit schedule will then be given to you, with first audits beginning no sooner than 1 year after your go live date

6.1 Consent: Identify a point of contact that will be responsible for working with Healthix and ensuring that your organization completes a state mandated consent audit.
The consent audit is conducted using the Healthix online consent audit tool. You will receive instructions on how to complete the tool. You must also send Healthix a copy of the consent form you have stored at your facility for each patient shown in the consent audit tool. Healthix will evaluate the information you give in the consent tool against the copies of the consent forms you send and produce a consent audit report for your records. Depending on your audit score, you may be required to perform some remediation. Remediation requirements vary with score ranges.

6.2 User: Identify a point of contact that will be responsible for working with Healthix and ensuring that your organization completes a bi-annual user audit. The purpose of the audit is to ensure that the information and permissions Healthix has for your authorized users is accurate and up-to-date. You will receive a report of all your authorized users with active accounts. It will have blank fields for you to enter information and instructions to walk you through it.

6.3 **Break the Glass: This audit is only required for participants that routinely engage in emergency services. If your organization has to undergo a BTG audit, you need to identify a point of contact that will be responsible for working with Healthix and ensuring that your organization completes the audit.

6.4 One to One Exchange: Identify a point of contact that will be responsible for working with Healthix. A participant in a One to One exchange agrees to be audited on a regular basis by Healthix to 1) validate proper authorization between parties, 2) validate patient/member relationship with providers and 3) proper level use of the PHI within the receiving provider

6.5 Participant List: Identify a point of contact that will be responsible for working with Healthix to validate receipt of the updated Healthix Participant List.

6.6 Annual HIPAA Training: Confirm that you provide annual HIPAA training to your employees. Healthix reserves the right to request you to produce such documentation, with reasonable notice.

6.7 Identity Proofing Identify a point of contact responsible for validating your identity proofing process. Healthix may require you to produce documentation for a sample of authorized Healthix users at your organization.

6.8 Qualified Service Organization Agreement (QSOA): Identify a point of contact that will be responsible for working with Healthix and ensuring that your organization completes a QSOA audit. Healthix generally conducts them on site, during which we will review your identity proofing process to confirm that the appropriate government issued ID is being used to validate an individual's identity.

NOTE: Healthix will continue to develop audits based on New York State mandates. We will assist you in preparation for any and all audits.

ACTION ITEMS *(date and initial that participant will be in full compliance before Healthix integration project is completed)*

1	Identify Contact for Consent Audit			
Full Name	Title	Phone #	email	
2	Identify Contact for the User audit			
Full Name	Title	Phone #	email	
3	Identify Contact to validate receipt of the updated Healthix Participant List			
Full Name	Title	Phone #	email	
4	Identify Contact for Break the Glass Audit			
Full Name	Title	Phone #	email	
5	Identify Contact for QSOA audit			
Full Name	Title	Phone #	email	
6	Confirm that you conduct annual HIPAA training		Date	Initials
7	Identify Contact for Compliance Matters			
Full Name	Title	Phone #	email	

Glossary of Exhibits:

Exhibit 1a: Consent Form – Without Emergency Services

Exhibit 1b: Consent Form – With Emergency Services

Exhibit 1c: Community-Wide Consent Form

Exhibit 2: Attestation

Exhibit 3: Healthix User Roles

Exhibit 4: BTG Signage

Exhibit 5: Definition of a 42 CFR Part 2 program

Exhibit 6: Patient Notice

Exhibit 7: Certified Application Requirements

Exhibit 8: One to One Exchange Authorizations (Provider to Provider, Health Plans, PPS)

Appendix:

1. [1] Including, but not limited to: HIPAA and HITECH, 42 C.F.R. Part 2, NY State Public Health Law, The NY State not for profit revitalization act, 10 N.Y.C.R.R. Section 300, and Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State v.3.1, available at (https://www.health.ny.gov/technology/regulations/shin-ny/docs/privacy_and_security_policies.pdf)

2. Required Language for Consent Form:

   Healthix-wide Denial of Consent: *If I want to deny consent for all Provider Organizations and Health Plans participating in Healthix to access my electronic health information through Healthix, I may do so by visiting Healthix's website at www.healthix.org or calling Healthix at 1-877-695-4749* ("I" can be changed to "you" for consistency with the rest of the form).

   Public Health and Organ Procurement Organization Access: Under the "Details about the information accessed through Healthix and the consent Process," the following sentence: *Federal, state or local public health agencies and certain organ procurement organizations are authorized by law to access health information without a patient's consent for certain public health and organ transplant purposes. These entities may access your information through Healthix for these purposes without regard to whether you give consent, deny consent or do not fill out a consent form.*