BronxRHIO
Connecting for Better Health

To:	Bronx RHIO Board of Directors & All Participant Organizations
From:	Charles Scaglione
Date:	October 28, 2021
Subject:	Recommended Changes to Bronx RHIO Policies and Procedures

The Bronx RHIO periodically updates its Participation Agreement, Member and Corporate Policies and Procedures, and Cybersecurity and Information System Management Program (CISMP) Policies and Plans to maintain compliance with SHIN-NY Policy Standards, HITRUST Certification requirements, and to address other laws, regulations and business requirements.

In consultation with counsel (Manatt) we are recommending an update to Bronx RHIO's Policies and Procedures. The revised Policies and Procedures will be effective October 28, 2021 and will become the new Exhibit A of your Participation Agreement.

The proposed changes (see attached redline) to Bronx RHIO's Policies and Procedures are to ensure alignment and conformance with Version 3.8.1 of New York State's Privacy and Security Policies and Procedures for Qualified Entities and their Participants.

Substantive changes consist of the following:

- Updating the definition of Emergency Medical Technician and providing that Emergency Medical Technicians may "break the glass" to access PHI outside of the emergency room provided that an emergency condition exists, the patient is in immediate need of medical care, and an attempt to secure consent would result in a delay of treatment which would increase the risk to the patient's life or health.
- Providing that the Bronx RHIO may disclose PHI without consent for purposes of determining a patient's cause of death not only to licensed physicians or nurse practitioners whose professional responsibilities include determining the cause of death of a patient, but also to individuals acting under the supervision of such physicians or nurse practitioners.
- Removing all gender-specific pronouns and other minor clarifying changes.

We recommend that the proposed changes be approved.

1776 Eastchester Rd., Suite 200, Bronx, NY 10461
Phone 718-708-6633 Fax 718-708-7272

Bronx RHIO, Inc.
Policies and Procedures

Definitions

1. ***Access*** means the ability of an Authorized User or Certified Application to view Protected Health Information through the RHIO System following the Authorized User's or Certified Application's logging on to the RHIO System.

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

3. ***Actors*** means Health Care Providers, Health IT developers of Certified Health IT, and Health Information Networks (HIN)/Health Information Exchanges (HIE), as each such term is defined in the Information Blocking Rules.

~~4. ***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.~~

~~5.~~4. ***Affiliated Practitioner*** means (i) a Practitioner employed by or under contract to a Provider Organization to render health care services to the Provider Organization's patients; (ii) a Practitioner on a Provider Organization's formal medical staff or (iii) a Practitioner providing services to a Provider Organization's patients pursuant to a cross-coverage or on-call arrangement.

~~6.~~5. ***Affirmative Consent*** means the consent of a patient obtained through the patient's execution of the Bronx RHIO consent form(s).

~~7.~~6. ***Alternative Consent*** means a consent form approved under Section 1.3 as an alternative to a Level 1 Consent or a Level 2 Consent.

~~8.~~7. ***Applicant*** means any healthcare facility or provider that wishes to become a Participant of the Bronx RHIO.

~~9.~~8. ***Application for Participation*** means an Applicant's application to become a Participant of the Bronx RHIO, in the form developed by the Bronx RHIO.

~~10.~~9. ***Audit Log*** means an electronic record of the Disclosure of information via the RHIO System, such as, for example, queries made by Authorized Users, type of

information Disclosed, information flows between the Bronx RHIO and Participants, and date and time markers for those activities..

~~11.~~10. ***Authorized User*** means an employee or independent contractor of a Participant or a credentialed member of the Participant's professional staff who meets the criteria set forth in Policy and Procedure 1-4 (Authorized Users) and has been authorized by the Participant to Access Protected Health Information through the RHIO System.

~~12.~~11. ***Authorized User Registration Form*** means the registration form required by the Bronx RHIO from Participants utilizing the Bronx RHIO's central authentication system (as opposed to a local authentication system) in order to load an Authorized User into the authentication system, including the name of the Authorized User and the level of access to the RHIO System such Authorized User will have.

~~13.~~12. ***Board of Directors*** is the Board of Directors of the Bronx RHIO, which consists of the individuals officially designated by the Members as their representatives on the Board of Directors.

~~14.~~13. ***Breach*** means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the Protected Health Information. An acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Participant or the Bronx RHIO can demonstrate that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the Protected Health Information or to whom the disclosure was made; (iii) whether the Protected Health Information was actually acquired or viewed; and (iv) the extent to which the risk to the Protected Health Information has been mitigated. Breach excludes: (i) any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of the Bronx RHIO 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 Protected Health Information at the Bronx RHIO or a Participant to another person authorized to access Protected Health Information at the Bronx RHIO 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 Protected Health Information where the Bronx RHIO 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.

~~15.~~14. ***Break the Glass*** means the ability of an Authorized User to Access a patient's Protected Health Information, in accordance with Section 1-3(III) (E) of these Policies and Procedures, without obtaining Affirmative Consent.

~~16.~~15. ***Bronx RHIO Research Committee*** means the Bronx RHIO committee that is organized to review and approve Research proposals. The Bronx RHIO will ensure that the committee meets the requirements set forth at 45 C.F.R. § 164.512(i)(1)(i)(B), meaning that the committee (1) has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the Research protocol on individuals' privacy rights and related interests; (2) includes at least one member who is not an employee, contractor, officer or director of the Bronx RHIO or any entity conducting or sponsoring the research, and is not related to any person who meets any of the foregoing criteria; and (3) does not have any member participating in a review of any project in which the member has a conflict of interest.

~~17.~~16. ***Care Management*** means (i) assisting a patient in obtaining appropriate medical care, (ii) improving the quality of health care services provided to a patient, (iii) coordinating the provision of multiple health care services to a patient; (iv) supporting a patient in following a plan of medical care, or (v) assisting a patient in obtaining social services or providing social services to a patient. Care Management does not include utilization review or other activities carried out by a Payer Organization to determine whether coverage should be extended or payment should be made for a health care service.

~~18.~~17. ***CARIN Alliance*** means the multi-sector collaborative that seeks to advance consumer-directed exchange of health information and which has developed a list of recommended Patient Apps via its "My Health Application" website.

~~19.~~18. ***Certified Application*** means a computer application certified by the Bronx RHIO that is used by a Participant to Access Protected Health Information from the Bronx RHIO on an automated, system-to-system basis without direct Access to the RHIO System by an Authorized User.

~~20.~~19. ***Community-Based Organization*** means an organization, which may be a not-for-profit entity or government agency, which has the primary purpose of providing social services such as housing assistance, nutrition assistance, employment assistance, or benefits coordination. A Community-Based Organization may or may not be a Covered Entity.

~~21.~~20. ***Coroner*** means any individual elected to serve as a county's coroner in accordance with New York State County Law § 400.

~~22.~~21. ***Covered Entity*** has the meaning ascribed to this term in 45 C.F.R. § 160.103.

~~23.~~22. ***Data Provider*** means an individual or entity that supplies information, including Protected Health Information to or through the Bronx RHIO. Data Providers

include both Participants and entities that supply but do not Access Protected Health Information via the SHIN-NY (such as clinical laboratories and pharmacies). Government agencies, including Public Health Agencies, may be Data Providers.

~~24.~~23. ***De-Identified Data*** means data that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Data may be considered de-identified only if it (i) satisfies the requirements of 45 C.F.R. § 164.514(b) and (ii) does not contain DNA variation information derived from sequencing, genotyping or other such technologies.

~~25.~~24. ***Demographic Information*** means a patient's name, gender, address, date of birth, social security number, and other personally identifiable information, but shall not include any information regarding a patient's health or medical treatment or the names of any Data Providers that maintain medical records about such patient.

~~26.~~25. ***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.

~~27.~~26. ***Disclosure*** means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. The Bronx RHIO engages in a Disclosure of information if the Bronx RHIO (i) provides a Participant with Access to such information and the Participant views such information as a result of such Access, or (ii) Transmits such information to a Participant or other third party.

~~28.~~27. ***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 State law.

28. ***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.

29. ***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 and 800.6 as an emergency medical technician, an emergency medical technician-intermediate, an emergency medical technician-critical care, or an emergency medical technician-paramedic.

26 ***Excluded Health Information*** means (i) psychotherapy notes and (ii) any other information that the Board of Directors of the Bronx RHIO determines may not be disclosed through the RHIO System under applicable law.

27. ***Exception*** means reasonable and necessary activities that do not constitute Information Blocking as set forth in the Information Blocking Rules, namely: 1. Preventing Harm 2. Privacy 3. Security 4 Infeasibility 5. Health IT Performance/Maintenance 6. Content and Manner 7. Fees 8. Licensing.

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

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

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

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

32. ***HIPAA*** means the Health Insurance Portability and Accountability Act of 1996.

33. ***HIPAA Privacy Rule*** means the federal regulations at 45 CFR Part 160 and Subparts A and E of Part 164.

34. ***HIPAA Security Rule*** means the federal regulations at 45 CFR Part 160 and Subpart C of Part 164.

35. ***HITECH*** means the Health Information Technology for Economic and Clinical Health Act.

36. ***Independent Practice Association*** ("IPA") means an entity that is certified as an independent practice association under 10 N.Y.C.R.R. § 98-1.5(b)(6)(vii).

37. ***Information Blocking*** means a practice that except as required by law or covered by an Exception is likely to interfere with access, exchange, or use of electronic health information, if 1) conducted by a health information technology developer, health information network (HIN) or health information exchange (HIE) when such Actor knows or should have known that such practice is likely to interfere with access, exchange, or use of electronic health information (EHI), or if 2) conducted by a healthcare provider when such Actor knows that such practice is unreasonable and is likely to interfere with access, exchange, or use of EHI.

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

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

41. ***Level 1 Consent*** means a consent permitting Access to and receipt of Protected Health Information for Level 1 Uses in one of the forms attached to the QE Privacy & Security Policies & Procedures.

42. ***Level 2 Consent*** means a consent permitting Access to and receipt of Protected Health Information for a Level 2 Use in one of the forms attached to the QE Privacy & Security Policies & Procedures.

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

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

45. ***Limited Data Set*** means Protected Health Information that excludes the 16 direct identifiers set forth at 45 C.F.R. § 164.514(e)(2) of an individual and the relatives, employers or household members of such individual.

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

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

48. ***Members*** are the corporate members of the Bronx RHIO, as defined in the Bylaws of the Bronx RHIO.

49. ***Minor Consent Information*** means Protected Health Information relating to Minor Consented Services.

50. ***Minor Consented Services*** means medical treatment of a minor for which the minor provided ~~his or her~~ the minor's 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, sexually transmitted disease, mental health or substance abuse treatment) or services consented to by an Emancipated Minor.

51. ***NYS DOH*** means the New York State Department of Health.

52. ***Organ Procurement Organization*** means a regional, non-profit organization responsible for coordinating organ and tissue donations at a hospital that is

designated by the Secretary of Health and Human Services under section 1138(b) of the Social Security Act (42 USC § 1320b-8(b); see also 42 C.F.R. Part 121).

53. ***Participant*** means a Provider Organization, Payer Organization, Practitioner, Independent Practice Association, Accountable Care Organization, Public Health Agency, Organ Procurement Organization, Health Home, Health Home Member, PPS Lead Organization, PPS Centralized Entity, PPS Partner, Social Services Program, a Community-Based Organization or Disaster Relief Agency that has directly or indirectly entered into a Participation Agreement and Accesses Protected Health Information through the RHIO System.

54. ***Participation Agreement*** is the agreement made by and between the Bronx RHIO and each Participant, which sets forth the terms and conditions governing the operation of the RHIO System and the rights and responsibilities of the Participants and the Bronx RHIO with respect to the RHIO System.

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

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

57. ***Patient Rights and Member Responsibilities Committee*** means the committee of the Bronx RHIO that is responsible for monitoring compliance with these Policies and Procedures.

58. ***Payer Organization*** means an insurance company, health maintenance organization, employee health benefit plan established under the Employee Retirement Income Security Act or any other entity that is legally authorized to provide health insurance coverage.

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

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

61. ***PPS*** means a Performing Provider System that has received approval from NYS DOH to implement projects and receive funds under New York's Delivery System Reform Incentive Payment Program (DSRIP).

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

63. ***PPS Lead Organization*** means an entity that has been approved by NYSDOH and CMS to serve as designated organization that has assumed all responsibilities associated with DSRIP program per their project application and DSRIP award.

64. ***PPS Partner*** means a person or entity that is listed as a PPS Partner in the DSRIP Network Tool maintained by NYS DOH.

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

66. ***Protected Health Information*** means information maintained or transmitted by a Participant that (i) relates to the present, past or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present, or future payment for the provision of health care to an individual and/or (ii) identifies the individual, or with respect to which, there is a reasonable basis to believe the information can be used to identify the individual, including, without limitation, student or employment records.

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

68. ***Public Health Agency*** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, an Indian tribe, the New York State Department of Health, a New York county health department or the New York City Department of Health and Mental Hygiene, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate and that has signed a Participation Agreement with the Bronx RHIO and Accesses Protected Health Information through the RHIO System.

69. ***"Qualified Entity" or "QE"*** means a not-for-profit regional health information organization or other entity that has been certified under 10 N.Y.C.R.R. Section 300.4.

70. ***Quality Improvement*** means activities designed to improve processes and outcomes related to the provision of health care services. Quality Improvement activities include but are not limited to outcome evaluations; development of clinical guidelines; population based activities relating to improving health or reducing health care costs; clinical protocol development and decision support tools; case management and care coordination; reviewing the competence or qualifications of health care providers, but shall not include Research. The use or Disclosure of Protected Health Information for quality improvement activities may be permitted provided the Accessing and Disclosing entities have or had a relationship with the individual who is the subject of the Protected Health Information.

71. ***QE Privacy & Security Policies & Procedures*** means the "Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 NYCRR § 300.3(b)(1)" developed through the Statewide Collaboration Process and approved by NYS DOH setting forth the common consent, authorization, authentication, access, patient engagement and access, audit, and breach policies with which Qualified Entities must comply.

72. ***Record Locator Service or Other Comparable Directory*** means a system, queriable only by Authorized Users, that provides an electronic means for identifying and locating a patient's medical records across Data Providers.

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

74. ***Retrospective Research*** means Research that is not conducted in connection with Treatment and involves the use of Protected Health Information that relates to Treatment provided prior to the date on which the Research proposal is submitted to an Institutional Review Board.

75. ***RHIO Staff*** means those individuals who are employed or contracted by the Bronx RHIO for the purpose of carrying out the functions of the Bronx RHIO.

76. ***RHIO System*** means the clinical information data exchange operated by the Bronx RHIO.

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

78. ***Statewide Health Information Network for New York or SHIN-NY*** means the means the technical infrastructure (SHIN-NY Enterprise) and the supportive policies and agreements that make possible the electronic exchange of clinical information among QEs, Participants, and other individuals and entities for authorized purposes, including both the infrastructure that allows for exchange among Participants governed by the same QE and the infrastructure operated by the State Designated Entity that allows for exchange between different QEs. The goals of the SHIN-NY are to improve the quality, coordination and efficiency of patient care, reduce medical errors and carry out public health and health oversight activities, while protecting patient privacy and ensuring data security.

79. ***SHIN-NY Enterprise*** means the information technology (IT) infrastructure inclusive of the QEs and the statewide SHIN-NY Hub that supports the electronic exchange of patient health information across New York State.

80. ***SHIN-NY Hub*** means the information technology (IT) infrastructure operated by the State Designated Entity that allows for the exchange of information between QEs.

~~81. ***SHIN-NY Portal*** means the secure online website that gives patients and their Personal Representatives access to the Protected Health Information about them that is available through the SHIN-NY.~~

~~82.~~81. ***Social Services Program*** means a program within a social services district (as defined by New York Social Services Law, § 2) which has authority under applicable law to provide "public assistance and care" (as defined by New York Social Services Law § 2), Care Management, or coordination of care and related services.

~~83.~~82. ***State Designated Entity ("SDE")*** means the public/private partnership in New York State that has been designated by the New York State Commissioner of Health as eligible to receive federal and state grants to promote health information technology.

~~84.~~83. ***Statewide Collaboration Process ("SCP")*** means an open, transparent process within which multiple SHIN-NY stakeholders contribute to recommendations for SHIN-NY Policy Guidance as provided in 10 N.Y.C.R.R. Section 300.3.

~~85.~~84. ***Telehealth*** means the use of electronic information and two-way, real-time communication technologies to deliver health care to patients at a distance. Such communication technologies include both audio-video and audio-only (e.g., telephonic) connections.

~~86.~~85. ***Training*** means the instructions in the use of the RHIO System, as well as in the policies and procedures governing that use, that will either be provided by the Bronx RHIO to designated individuals at each site, designated individuals who in turn will be training users at each site, or that will be available via the web for

self-paced learning, as more fully described in the Policy and Procedure on Training.

~~87.~~86. ***Transmittal*** means the Bronx RHIO's transmission of Protected Health Information, a Limited Data Set, or De-identified Data to a recipient in either paper or electronic form, other than via the display of such information through the RHIO System or through a Certified Application.

~~88.~~87. ***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.

~~89.~~88. ***Unsecured Protected Health Information*** means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services in guidance issued under section 1 3402(h)(2) of HITECH (42 USC 1 7932(h)(2)).

~~90.~~89. ***User Authentication*** means the procedure established to assure that each Authorized User is identified and the validity of such Authorized User's credentials is established before such Authorized User is granted access to the RHIO System.

Bronx RHIO, Inc.
Policy and Procedure
1-1
Adoption of Policies and Procedures

Originally Adopted May 14, 2007
Amended and Restated April 26, 2018

I. Policy

It is the policy of the Bronx RHIO to bring all corporate policies and procedures governing the operation of the RHIO System to the Board of Directors for review and approval by a majority vote.

II. Responsible Parties

The Executive Director is responsible for the development of policies and procedures governing the operation of the RHIO System (the "Policies and Procedures"), including the development of proposed amendments to the Policies and Procedures when necessary.

Committees of the Board are responsible for reviewing draft Policies and Procedures and proposed amendments to the Policies and Procedures and making a recommendation to the Board of Directors as to whether they should be adopted by the Board.

The Board of Directors is responsible for reviewing draft Policies and Procedures and proposed amendments to the Policies and Procedures and determining if they should be adopted by the Board of Directors. Participants (including Members) are responsible for complying with the Policies and Procedures once they are adopted by a majority vote of the Board of Directors.

III. Procedure

A. The Executive Director, working with staff or Board and Committee members as necessary, will periodically review the Policies and Procedures and make recommendations for amendments, if necessary.

B. The proposed amendments to the Policies and Procedure may be presented to a Committee if they are relevant to the charge of that Committee for review and recommendation for action to the Board or may be brought directly to the Board of Directors for consideration.

C. Proposed amendments to the Policies and Procedures will be circulated to the Board and Committee members no less than one week prior to the scheduled date of the meeting where voting will take place.

D. No Policies and Procedures will be adopted or amended other than by majority vote of the Board of Directors.

E. Once a Policy and Procedure is adopted or amended it will be incorporated into the Participation Agreement in accordance with and subject to the provisions regarding the establishment of Policies and Procedures set forth in the Participation Agreement.

F. Policies and Procedures may only be adopted or amended by majority vote of the Board of Directors.

Bronx RHIO, Inc.
Policy and Procedure
1-2
Participation in the Bronx RHIO

Originally Adopted February 25, 2008
Amended and Restated as of June 30, 2014
Amended and Restated as of June 27, 2019
Amended and Restated as of June 30, 2020
Amended and Restated as of April 29, 2021

I. Policy

It is the policy of the Bronx RHIO to obtain the approval of the Board of Directors of the Application for Participation of each Applicant prior to permitting such Applicant to Access or receive Protected Health Information through the RHIO System.

II. Responsible Parties

The Executive Director of the Bronx RHIO is responsible for assuring that each Applicant has submitted its Application for Participation and that the Board of Directors has approved such Application for Participation prior to permitting such Applicant to Access or receive Protected Health Information through the RHIO System.

Applicants are responsible for completing the Application for Participation, the Participation Agreement, the Participant Risk Assessment, and paying any applicable fees.

III. Procedures

A. Bronx RHIO will utilize a participant onboarding plan to define and document the participation process.

B. Prior to becoming a Participant and being authorized to Access or receive Protected Health Information through the RHIO System, each Applicant must complete an Application for Participation which will be submitted to the Board of Directors for consideration.

C. Approval of an Applicant's Application for Participation requires a majority vote of the entire Board of Directors.

D. Approval to participate requires agreement by the Participant to meet the minimum requirements for the category or categories in which they are applying.

E. A Participant may request a change in the level of participation by submitting a written request to the Bronx RHIO. Such requests shall be subject to the approval of the Executive Director.

F. The Participant will keep its list of participating facilities and/or sites up to date and will notify the Bronx RHIO of any changes in its organizational makeup.

G. Prior to Accessing or receiving Protected Health Information through the RHIO System, each Participant must sign a Participation Agreement.

H. As part of the Application for Participation, each Participant must complete a Participant Risk Assessment ("PRA"). The PRA allows the Bronx RHIO to assess, identify, and modify the overall security position of the organization and its risks to Protected Health Information. Failure to return a completed PRA may delay the application process and participation in the Bronx RHIO.

1. Every two (2) years, on the anniversary of the effective date of the Participation Agreement, a Participant shall be required to submit a new PRA. From time to time in between submission of PRAs, the Bronx RHIO may require a Participant to provide an Attestation of Security Compliance Form, attached here as Attachment A. Should the information in the previously submitted PRA require updates, the Participant must submit a new PRA, and not an Annaul Attestation Form.The RHIO will use reasonable efforts to secure a completed PRA from those Participants who joined the RHIO prior to its adoption.

Attachment A

Attestation of Security Compliance Form

_____ ("Participant") has entered into a Participation Agreement with Bronx RHIO ("RHIO") on _____. Participant returned a Participant Risk Assessment to RHIO, which was received on _____. This Attestation of Security Compliance is provided by Participant in accordance with the RHIO Policies and Procedures.

Participant attests to RHIO that it has reviewed the most recently submitted Participant Risk Assessment, its internal process and policies, service providers, vendors, agents, and other providing services, and the following statements are accurate as of the date hereof:

1. Any and all risks to Protected Health Information, including, without limitation, any discovered vulnerabilities or gaps, have been mitigated in a manner supported by industry standards.
2. Participant has reviewed the RHIO Policies and Procedures, and to the extent necessary and appropriate to comply with applicable law and RHIO Policies and Procedures, Participant has revised its policies and procedures.
3. All training with respect to access and use of the Protected Health Information has been documented, and training occurs before any employee, representative, or agent may access the RHIO system.
4. All disposed media that stored Protected Health Information has been properly destroyed and documented, in accordance with the Participation Agreement.
5. Participant has reported to RHIO all security incidents, including but not limited to a Breach, as required by the Participation Agreement and RHIO Policies and Procedures.
6. The most recently submitted Participant Risk Assessment is accurate, and the information contained within requires no updates.

Participant

By: _____
Authorized Officer

Date: _____

Bronx RHIO, Inc.
Policy and Procedure
1-3
Privacy Policy & Procedure

Originally Adopted February 25, 2008
Amended and Restated as of September 18, 2015
Amended and Restated as of February 28, 2017
Amended and Restated as of September 25, 2017
Amended and Restated as of April 26, 2018
Amended and Restated as of June 27, 2019
Amended and Restated as of October 29, 2020
Amended and Restated as of April 29, 2021
Amended and Restated as of October __, 2021

I. Policy

It is the policy of the Bronx RHIO to require that all Participants or other Actors comply with state and federal laws and regulations related to the use and Disclosure of Protected Health Information, and comply with the Information Blocking Rules, which implement the provisions of the 21th Century Cures Act on data sharing compliance and prohibition on Information Blocking, as well as with the QE Privacy & Security Policies & Procedures and all privacy and security policies of the Bronx RHIO.

It is the policy of the Bronx RHIO to ensure that appropriate operational and technical safeguards exist to prevent the improper use and Disclosure of Protected Health Information. It is the policy of the Bronx RHIO that Participants respect a patient's right to withhold, from the patient's Payor Organization, Protected Health Information about services for which the patient pays out of pocket.

In the same way Participants currently have the responsibility to safeguard Protected Health Information contained in records within their facility, they will have the responsibility not to use or Disclose information obtained through the Bronx RHIO inappropriately.

II. Responsible Parties

The Board of Directors of the Bronx RHIO will have primary responsibility for overseeing the execution and revision of this privacy policy and for ensuring audits occur and that results and corrective actions are reported to the Board.

The Executive Director will oversee the activities of the Bronx RHIO to evaluate compliance by Participants with this policy and enforce its terms.

Participants will have responsibility for ensuring compliance with this policy at their sites.

III. Procedure

A. Consent

1. Each Participant will, as part of the patient admission or registration process, seek to obtain an Affirmative Consent permitting the Participant to Access or receive the patient's Protected Health Information through the RHIO System. Except as otherwise provided in these Policies, the Bronx RHIO shall not Disclose a patient's Protected Health Information to a Participant unless the patient has provided an Affirmative Consent authorizing the Participant to Access or receive such Protected Health Information. No Participant may modify the terms of the Affirmative Consent without the prior written approval of the Executive Director of the Bronx RHIO.

2. Once a Participant has obtained Affirmative Consent, or has obtained an affirmative denial of consent from a patient, the Participant will be responsible for recording the patient's consent status either in its internal registration system for automatic transmission to the RHIO System or directly into the RHIO System. Participants may not deny or restrict Treatment to a patient due to the patient's refusal to execute an Affirmative Consent nor due to the patient's affirmative denial of consent.

3. Affirmative Consents may not designate that some Protected Health Information may be Disclosed through the RHIO System, while other information will not. If a patient specifies he/she does not wish to have particular Protected Health Information Disclosed through the RHIO System, all information on that patient will be blocked from view through the RHIO System.

4. In no event, even if a patient has provided an Affirmative Consent, may Excluded Health Information be Disclosed through the RHIO System.

5. At the time a Participant seeks to obtain an Affirmative Consent from a patient, the Participant shall:

a. Provide the patient with a list or reference to all Data Providers participating in the RHIO at such time, information about how to contact Data Providers, an acknowledgement that Data Providers may change over time, and instructions for the patient to access an up-to-date list of Data Providers through the Bronx RHIO website or other means;

b. Provide the patient with notice – in a manner easily understood by patients – that their Protected Health Information is being uploaded to the Bronx RHIO, if applicable; and

c. Provide the patient with a description of how patients may deny consent for all Participants to Access their Protected Health Information through the Bronx RHIO.

d. If the Affirmative Consent authorizes the Participant to Access Protected Health Information for the purpose of Marketing, provide the patient with information about the nature of such Marketing.

6. An Affirmative Consent obtained by a Participant shall apply to an Affiliated Practitioner of the Participant provided that (i) such Affiliated Practitioner is providing health care services to the patient at the Participant's facilities; (ii) such Affiliated Practitioner is providing health care services to the patient in ~~his or her~~the Affiliated Practitioner's capacity as an employee or contractor of the Participant or (iii) such Affiliated Practitioner is providing health care services to the patient in the course of a cross-coverage or on-call arrangement with the Participant or one of its Affiliated Practitioners.

7. 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. See Electronic Signatures and Records Act (State Technology Law Article III, 9 NYCRR Part 540, New York State Office of Information Technology Services ESRA Guidelines NYS-G04-001).

B. User Access Control

1. Protected Health Information obtained by an Authorized User through the RHIO System may be used or Disclosed by the Authorized User only for the purposes set forth on the applicable Affirmative Consent.

2. Each Participant is responsible for training all of its Authorized Users on compliance with this policy, the QE Privacy & Security Policies & Procedures, the HIPAA regulations, other applicable privacy laws and rules, and the Participant's privacy and security policies.

3. Consistent with Section 1-15 of these Policies and Procedures, each Participant shall be responsible for disciplining any of its Authorized Users who violate the terms of this policy, the QE Privacy & Security Policies & Procedures, HIPAA or other applicable laws and regulations in accordance with its own policies and procedures and any guidelines that may be adopted by majority vote of the Board of Directors. Notwithstanding the foregoing, the Bronx RHIO reserves the right, in its sole discretion, to terminate (or cause the applicable Participant to terminate) the access to the RHIO System of any Authorized User who violates the terms of this policy, the QE Privacy & Security Policies & Procedures, HIPAA or other applicable laws and regulations.

4. The Board of Directors, through its Patient Rights and Member Responsibilities Committee, will be responsible for ongoing review of audits of the use and Disclosure of Protected Health Information through the RHIO System by each Participant and its Authorized Users.

5. The Bronx RHIO and its Participants will conduct periodic audits of appropriate Access to Protected Health Information in accordance with Policy and Procedure 1-7 (Audits).

C. Business Associate Agreements

1. The Bronx RHIO will ensure that all its contracts and contracts of any subcontractors include Business Associate Agreements to the extent required by Section 13408 of HITECH and 45 C.F.R. § 164.502(e).

2. The Bronx RHIO will enter into a Business Associate Agreement with each Data Provider that is a Covered Entity.

3. The Bronx RHIO will not use or Disclose Protected Health Information in any manner that violates the Bronx RHIO's Business Associate Agreements.

D. Minors' Records

1. Except as otherwise set forth in this Section D, a Participant may Access or receive Protected Health Information about minors

based on an Affirmative Consent executed by the minor's Personal Representative.

2. To ensure that Minor Consent Information is not inadvertently Disclosed by an Authorized User to a minor's parent or guardian based on the parent or guardian's Affirmative Consent, the RHIO System highlights a minor's records in yellow, and displays the following warning to Authorized Users upon login to the RHIO System: "The records that you are about to access may contain information related to Minor Consented Services. Re-disclosure of this information without the minor's consent to the minor's parents or guardians is generally prohibited by NY State laws and regulations with which you must comply."

3. To ensure that Minor Consent Information that is protected under 42 C.F.R. Part 2 is not Disclosed to any third party, including a parent or guardian, without the Affirmative Consent of the minor, the Bronx RHIO excludes any such data from Disclosure through the RHIO System.

4. Participants with concerns about Disclosure of their Minor Consent Information because they serve a population consisting primarily of minors may request a waiver from uploading their data to the Bronx RHIO from NYS DOH.

5. An Authorized User who is providing Minor Consented Services to a minor may Access the minor's Protected Health Information absent the Affirmative Consent of the minor's parent or guardian if the minor executes a Minor Consent Over-ride Form.

E. Emergency Disclosures of Protected Health Information When Treating a Patient with an Emergency Condition or "Breaking the Glass"

1. Affirmative Consent shall not be required for the Bronx RHIO to Disclose Protected Health Information to an Authorized User that is a Practitioner, an Authorized User that is acting under the direction of a Practitioner, or an Authorized User that is an ~~Advanced~~ Emergency Medical Technician, and these individuals may Break the Glass, if the following conditions are met:

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

b. The Practitioner or ~~Advanced~~ Emergency Medical Technician determines, in ~~his or her~~such individual's reasonable judgment, that information that may be held by or accessible through the Bronx RHIO may be material to emergency treatment (the individual "Breaking the Glass" may do so in a facility, an ambulance, or another location, provided that such individual accesses Protected Health Information only after the determination in paragraph (a), above, has been made);

c. No denial of consent to Access or receive the patient's information is currently in effect with respect to the Participant with which the Authorized User is affiliated;

d. In the event that an Authorized User acting under the direction of a Practitioner Breaks the Glass, such Authorized User records the name of the Practitioner providing such direction; and

e. The Authorized User that is a Practitioner, Authorized User that is acting under the direction of a Practitioner, or ~~Advanced~~ Emergency Medical Technician attests that all of the foregoing conditions have been satisfied.

2. Emergency Protected Health Information Access by an Authorized User acting under the direction of a Practitioner must be granted by the Practitioner on a case by case basis.

3. Any Access by an Authorized User to Protected Health Information pursuant to the procedures set forth in this Section E will be subject to an audit trail function that allows tracking and auditing of such Access.

4. Each Participant must ensure that any Disclosures pursuant to the procedures set forth in this Section E do not occur after the completion of treatment of the emergency condition.

5. Notwithstanding anything to the contrary in these Policies and Procedures, the Bronx RHIO and its Participants shall not be required to exclude any Sensitive Health Information from Disclosure where the circumstances set forth in this Section E are met.

6. If the Bronx RHIO includes data protected under 42 C.F.R. Part 2, the Bronx RHIO shall promptly notify Data Providers that are federally-assisted alcohol or drug abuse programs when Protected Health Information from the Data Provider's records is Disclosed

under this Section E. This notice shall include (i) the name of the Participant that received the Protected Health Information; (ii) the name of the Authorized User within the Participant that received the Protected Health Information; (iii) the date and time of the Disclosure; and (iv) the nature of the emergency.

7. ~~Upon a patient's discharge from a Participant's emergency room, if emergency Disclosure of Protected Health Information occurred during the emergency room visit~~If a Participant accesses Protected Health Information under this Section E, the Participant shall notify the patient of such incident and inform the patient how ~~he or she~~the patient may request an Audit Log of such Disclosure. In lieu of providing such notice, Participants that are hospitals may notify all patients discharged from an emergency room that their Protected Health Information may have been Disclosed during a Break the Glass incident and inform patients how they may request an Audit Log to determine if such Disclosure occurred. The notice required by this Section shall be provided within ten days of the patient's discharge, or, in the case of access that does not relate to a hospital admission, within ten days of the date of such access.

F. Other Privacy and Security Practices

1. Each Participant shall install, maintain and update on all of its computers used for the purpose of Accessing or receiving Protected Health Information through the RHIO System virus protection software that meets minimum standards established by the Bronx RHIO.

2. Each Participant shall promptly notify the Bronx RHIO of any use or Disclosure of Protected Health Information in violation of this policy or any related Breach of which it becomes aware. Each Participant shall, in consultation with the Bronx RHIO, take reasonable steps to mitigate the potentially harmful effects of any such incident.

3. Each Participant shall adopt and implement any other privacy and security policies and procedures relating to the use, maintenance and Disclosure of Protected Health Information obtained through the RHIO System that are necessary to assure the Participant's compliance with HIPAA, and all other applicable confidentiality laws and regulations.

4. Any Disclosure by the Bronx RHIO of Protected Health Information to an Authorized User through the RHIO System will be subject to an audit trail function that allows tracking and auditing of such Disclosure.

5. Each Participant shall keep confidential any Protected Health Information obtained through the RHIO System and shall only re-disclose such Protected Health Information as authorized by law.

6. Prior to re-disclosing Sensitive Health Information, Participants shall implement systems to identify and denote Sensitive Health Information in order to ensure compliance with applicable state and federal laws and regulations governing re-disclosure of such information, including, but not limited to, those applicable to HIV/AIDS, alcohol and substance abuse information, and records of facilities licensed or operated by the New York State Office of Mental Health or the New York State Office for People With Developmental Disabilities.

7. The Bronx RHIO shall meet the following requirements with respect to warning statements:

    a. A warning statement that is viewed by Authorized Users whenever they are obtaining Access to or receiving Transmittals of records of federally-assisted alcohol or drug abuse programs regulated under 42 C.F.R. Part 2 that contains the language required by 42 C.F.R. § 2.32. The Bronx RHIO may satisfy this requirement by placing such a re-disclosure warning on all records that are made accessible through the RHIO.

    b. A warning statement that is viewed by Authorized Users whenever they are obtaining Access to or receiving Transmittals of HIV/AIDS information protected under Article 27-F of the N.Y. Public Health Law that contains the language required by Article 27-F (see Public Health Law 2782(5)). The Bronx RHIO may satisfy this requirement by (i) placing such a re-disclosure warning on the same screen on which it places the re-disclosure warning required at Section 7(a) above, or (ii) placing such a re-disclosure warning on a log-in screen that Authorized Users must view before logging into their EHR or otherwise Accessing the RHIO System.

    c. A warning statement that is viewed by Authorized Users whenever they are obtaining Access to or receiving Transmittals of records of facilities licensed or operated by the New York State Office of Mental Health or the New York State Office for People With Developmental Disabilities that contains language notifying the Authorized User that such records may not be re-disclosed except as permitted by the New York Mental Hygiene Law. The

Bronx RHIO may satisfy this requirement by (i) placing such a re-disclosure warning on the same screen on which it places the re-disclosure warning required at Section 7(a) above, or (ii) placing such a re-disclosure warning on a log-in screen that Authorized Users must view before logging into their EHR or otherwise Accessing the RHIO System.

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

e. The Bronx RHIO may note whether a patient has signed a MOLST or other advance directive in a Record Locator Service or Other Comparable Directory without Affirmative Consent.

G. Services Paid for Out of Pocket

1. If a patient pays for services out of pocket and requests that the Participant that provides such services not Disclose information relating to such services to the patient's Payor Organization, the Participant and the Bronx RHIO will follow the following procedures:

a. The Participant will advise the patient that if the Payor Organization is or becomes a Participant in the Bronx RHIO, and the patient signs an Affirmative Consent authorizing the Payor Organization to Access the patient's information through the RHIO System, the information available to the Payor Organization will include all of the patient's information that is available through the Bronx RHIO, since the RHIO System is not capable of blocking Access by a Payor Organization to information about specific services received by a patient from a specific Participant.

b. If the patient's Payor Organization is a Participant in the Bronx RHIO, which the Participant can confirm by checking the Bronx RHIO website, then the Participant will advise the patient that if the patient wishes to block Access

by that Payor Organization to information about specific services received by a patient from a specific Participant, the patient must block all Access by the Payor Organization to the patient's information, and that this can be done by completing the No Access for Health Plan consent form ("No Access Form").

c. If the patient completes the No Access Form, the Participant will forward the completed form to the Bronx RHIO, and the Bronx RHIO will block all Access by the Payor Organization to the patient's information.

d. The Bronx RHIO will notify the Payor Organization of the patient's decision and will provide the Payor Organization with a copy of the No Access Form for the Payor Organization's records.

e. If the Payor Organization is not currently a Participant in the Bronx RHIO, the Participant will advise the patient that if their Payor Organization becomes a Participant in the Bronx RHIO, the Payor Organization will need the patient to sign an Affirmative Consent in order for the Payor Organization to be able to Access the patient's data. The patient has the right not to sign an Affirmative Consent, and if the patient does not sign an Affirmative Consent, the Payor Organization will not have Access to any information about the patient through the Bronx RHIO, including information about services that the patient paid for out-of-pocket.

H. Access by the Bronx RHIO for Operations and Other Purposes.

1. Affirmative Consent is not required for the Bronx RHIO or its contractors to Access or receive Protected Health Information via the RHIO System and the SHIN-NY to enable the Bronx RHIO to perform system maintenance, testing and troubleshooting and to provide similar operational and technical support.

2. Affirmative Consent is not required for the Bronx RHIO or its contractors to Access or receive Protected Health Information via the RHIO System and the SHIN-NY 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 or receipt must be consistent with the terms of the Business Associate Agreement entered into by the Participant and the Bronx RHIO.

3. Affirmative Consent is not required for the Bronx RHIO or its contractors to Access or receive Protected Health Information via the RHIO System and the SHIN-NY for the purpose of evaluating and improving RHIO operations.

I. Access by Government Agencies. Notwithstanding anything to the contrary set forth in these Policies and Procedures, Affirmative Consent shall not be required for government agencies or their contractors to Access or receive Protected Health Information via the RHIO System and the SHIN-NY for the purpose of evaluating and improving RHIO operations.

J. Public Health Reporting and Access.

1. The Bronx RHIO may Disclose Protected Health Information to a Public Health Agency without Affirmative Consent for public health activities authorized by law, including:

a. To investigate suspected or confirmed cases of communicable disease (pursuant to PHL § 2(1)(1) and 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. As authorized by PHL § 206(1)(d) to investigate the causes of disease, epidemics, the sources of mortality, and the effect of localities, employments and other conditions, upon the public health, and by PHL § 206(1)(j) for scientific studies and research which have for their purpose the reduction of morbidity and mortality and the improvements of the quality of medical care through the conduction of medical audits;

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

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

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

h. For the activities of the Electronic Clinical Laboratory Reporting System (ECLRS), the Electronic Syndromic Surveillance System (ESSS) and the Health Emergency Response Data System (HIERDS);

i. For purposes allowed by PHL § 2004 and 10 N.Y.C.R.R. Part 62 (Alzheimer's);

j. For purposes allowed by PHL § 2819 (infection reporting);

k. For quality improvement and quality assurance under PHL Article 29-D, Title 2, including quality improvement and quality assurance activities under PHL § 2998-e (office-based surgery);

l. For purposes allowed under 10 N.Y.C.R.R. Part 22 (environmental diseases);

m. To investigate suspected or confirmed cases of lead poisoning (pursuant to 10 N.Y.C.R.R. Part 67);

n. For purposes allowed by 10 N.Y.C.R.R. Part 69 (including newborn disease screening, newborn hearing screening and early intervention);

o. For purposes allowed under 10 N.Y.C.R.R. § 400.22 (Statewide Perinatal Data System);

p. For purposes allowed under 10 N.Y.C.R.R. § 405.29 (cardiac data); or

q. For any other public health activities authorized by law. "Law" means a federal, state or local constitution, statute, regulation, rule, common law, or other governmental action having the force and effect of law, including the Charter, Administrative Code and Rules of the City of New York.

2. A patient's denial of consent for all Participants in the Bronx RHIO to Access the patient's Protected Health Information under Section A(5)(c) shall not prevent or otherwise restrict the Bronx RHIO from Disclosing to a Public Health Agency the patient's Protected Health Information through the RHIO System for the purposes set forth in Section J(1)(a)-(q).

3. The Bronx RHIO may Disclose the reports and information subject to 10 NYCRR §63.4 (HIV clinical laboratory test results), for purposes of linkage to and retention in care, to Participants engaged in Care Management that have a clinical, diagnostic, or

public health interest in the patient¸ to the extent permitted under 10 NYCRR §63.4(c)(3). Participants engaged in Care Management with a clinical, diagnostic, or public health interest in a patient may include, but are not limited to, Provider Organizations or Practitioners with a Treatment relationship with a patient, Health Homes, and Payer Organizations providing Care Management to their enrollees. The Bronx RHIO shall work in consultation with the New York State Department of Health, AIDS Institute, prior to implementing any program under this provision.

4. If a Data Provider or Participant is permitted to Disclose Protected Health Information to a government agency for purposes of public health reporting, including monitoring disease trends, conducting outbreak investigations, responding to public health emergencies, assessing the comparative effectiveness of medical treatments (including pharmaceuticals), conducting adverse drug event reporting, and informing new payment reforms, without patient consent under applicable state and federal laws and regulations, the Bronx RHIO may make that Disclosure on behalf of the Data Provider or Participant without Affirmative Consent.

K. Organ Procurement Organization Access. The Bronx RHIO may Disclose Protected Health Information to an Organ Procurement Organization without Affirmative Consent solely for the purposes of facilitating organ, eye or tissue donation and transplantation. A patient's denial of Affirmative Consent for all Participants in the Bronx RHIO to Access the patient's Protected Health Information under Section A(5)(c) shall not prevent or otherwise restrict an Organ Procurement Organization from Accessing or receiving the patient's Protected Health Information through the Bronx RHIO for the purposes set forth in this Section K.

L. De-Identified Data.

1. Disclosure of De-Identified Data for Specified Uses.

a. Affirmative Consent shall not be required for the Bronx RHIO to Disclose De-Identified Data for Research in accordance with Section Q.1.

b. Affirmative Consent shall not be required for the Bronx RHIO, a Participant, or a government agency to Access or receive De-Identified Data via the RHIO System for any purpose for which the Bronx RHIO, Participant, or government agency may lawfully Access or receive Protected Health Information under these Policies and Procedures.

c. Affirmative Consent shall not be required for the Bronx RHIO to Disclose De-Identified Data via the RHIO System for Quality Improvement, provided that a specially designated committee appointed by the Bronx RHIO reviews and approves the Quality Improvement activity in accordance with standards. Participants must make available to the committee the methodology of any proposed Quality Improvement project, which Bronx RHIO shall make accessible to other Participants and the general public.

d. Affirmative Consent shall not be required for the Bronx RHIO to perform an evaluation of the economic or other value of the Bronx RHIO provided that the methodology and results of any such evaluation are posted on the Bronx RHIO's website.

e. Affirmative Consent shall not be required for the Bronx RHIO to Transmit to a third party that is designing a clinical trial or other clinical research study a count of the number of patients who appear to meet the inclusion and/or exclusion criteria being considered for such clinical trial or study, so long as there is no reasonable basis to believe that the count, when combined with the qualifying criteria, can be used to identify an individual.

2. Creation of De-Identified Data for Specified Uses. The Bronx RHIO may Access Protected Health Information to create and validate the accuracy of De-Identified Data that is used in accordance with Section L(1).

3. Other Requirements.

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

b. The Bronx RHIO will not condition a patient's participation in the Bronx RHIO on the patient's decision to consent or deny Access to De-Identified Data for purposes other than those set forth in Section L(1).

c. The Bronx RHIO and its Participants will comply with standards for the de-identification of data set forth in 45 C.F.R. § 164.514.

d. The Bronx RHIO, its Participants and government agencies will subject any use of De-Identified Data to adequate restrictions on the re-identification of such data.

M. Consent for Access by ACOs, IPAs and Health Homes. An Affirmative Consent authorizing Access by an ACO, IPA or Health Home shall cover only the ACO, IPA or Health Home entity itself and not the health care providers participating in the ACO or IPA or Health Home.

N. Patient Care Alerts.

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

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

3. Patient Care Alerts shall be Transmitted in an encrypted form that complies with U.S. Health and Human Services Department Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

O. Access by Certified Applications. In the event that the Bronx RHIO permits Certified Applications to Access Protected Health Information through the RHIO System, such Access will be in accordance with the terms of these Policies and Procedures. The Bronx RHIO's certification process for Certified Applications will satisfy all encryption and other security standards incorporated into the SHIN-NY Policy Guidance.

P. Disclosures for Disaster Tracking

1. For the purpose of locating patients during an Emergency Event, the Bronx RHIO may Disclose to a Disaster Relief Agency the following information without Affirmative Consent:

    a. Patient name and other demographic information in accordance with the principles set forth in Section III.F of Policy and Procedure 1-4 (Authorized Users, Access to and Uses of Data); and

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

2. The Bronx RHIO may Disclose information under this section during an Emergency Event only.

3. Information Disclosed under this section shall not reveal the nature of the medical care received by the patient who is the subject of the Disclosure 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.

4. A patient's denial of consent for all Participants in the Bronx RHIO to Access or receive the patient's Protected Health Information shall not restrict the Bronx RHIO from Disclosing information to a Disaster Relief Agency as permitted in this section.

Q. Research

1. Research Involving De-Identified Data. Affirmative Consent shall not be required for the Bronx RHIO to Disclose De-Identified Data for purposes of Research, provided that the Bronx RHIO has adopted policies that inform Data Providers about the circumstances under which De-Identified Data may be Disclosed. The Disclosure of De-Identified Data under this section is subject to the Bronx RHIO's compliance with policies adopted by the Bronx RHIO, which set forth criteria that will be utilized to determine when a proposed Disclosure under this section must be approved by an Institutional Review Board or the Bronx RHIO Research Committee.

2. Research Involving a Limited Data Set. Affirmative Consent shall not be required for the Bronx RHIO to Disclose a Limited Data Set for purposes of Research, provided that (i) the Bronx RHIO has adopted policies that inform Data Providers about the

circumstances under which a Limited Data Set may be Disclosed; and (ii) the Bronx RHIO enters into a data use agreement with the researcher prior to Disclosing the Limited Data Set in accordance with the HIPAA Privacy Rule. The Disclosure of a Limited Data Set under this section is subject to the Bronx RHIO's compliance with policies adopted by the Bronx RHIO, which set forth criteria that will be utilized to determine when a proposed Disclosure under this section must be approved by an Institutional Review Board or the Bronx RHIO Research Committee.

3. Research Involving Protected Health Information.

a. Use of Protected Health Information for Patient Recruitment for Research. Affirmative Consent shall not be required for the Bronx RHIO to review Protected Health Information on behalf of a researcher to determine which individuals may qualify for a Research study. In addition, Affirmative Consent shall not be required for the Bronx RHIO to Disclose the name and other identifying information of an individual who may qualify for a Research study to a Participant that has a treating relationship with such individual so that the Participant may contact the individual to determine ~~his or her~~the individual's willingness to participate in such study, provided that all of the following requirements are met:

(1) an Institutional Review Board has approved of such Disclosure;

(2) the Bronx RHIO Research Committee has approved of such Disclosure;

(3) the Data Provider(s) that are the source of the Protected Health Information have agreed to allow for the Disclosure of their Protected Health Information for purposes of Research; and

(4) the Disclosure does not include any mental health clinical information governed by Section 33.13 of the Mental Hygiene Law, unless the recipient of the Disclosure is a facility as defined in the Mental Hygiene Law.

b. Use of Protected Health Information for Retrospective Research. Affirmative Consent shall not be required for the Bronx RHIO to Disclose Protected Health Information to a researcher conducting Retrospective Research if: (1) an

Institutional Review Board has approved of such Disclosure; (2) the Bronx RHIO Research Committee has approved of such Disclosure; and (3) the Data Provider(s) that are the source of the Protected Health Information have agreed to allow for Disclosures of their Protected Health Information for purposes of Research

4. Other Requirements Relating to Research. The Bronx RHIO shall not allow a Participant to opt out of having its Protected Health Information de-identified or converted into a Limited Data Set and used for Research that complies with paragraphs 1 or 2, above.

5. Research Committee. All applications for the Disclosure of Protected Health Information for Research shall be subject to the review and approval of the Bronx RHIO Research Committee.

R. Form of Patient Consents. Consents shall be obtained through a form approved by the Bronx RHIO. The Bronx RHIO may approve an alternative to a Level 1 Consent or a Level 2 Consent if the Alternative Consent includes the information specified in this Section R. The Bronx RHIO is responsible for ensuring that any approved Alternative Consents comply with applicable federal, state and local laws and regulations. If an Alternative Consent is to be used as a basis for exchanging information subject to 42 C.F.R. Part 2, the Bronx RHIO shall ensure that such form meets the requirements of 42 C.F.R. Part 2.

1. Level 1 Uses. Affirmative Consent to Access or receive information via the SHIN-NY for Level 1 Uses shall be obtained using a Level 1 Consent or an Alternative Consent approved by the Bronx RHIO under this Section R(1), which shall include the following information:

a. A description of the information which the Participant may Access or receive, including specific reference to HIV, mental health, alcohol and substance abuse, reproductive health, sexually-transmitted disease, and genetic testing information, if such categories of information may be Disclosed to the recipient;

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

c. The name(s) or description of both the source(s) and potential recipient(s) of the patient’s information. A general description, such as “information may be exchanged among

providers that provide me with treatment," shall meet this requirement; and

d. The signature of the patient or the patient's Personal Representative. If the consent language required under subsections (a), (b), and (c) above is incorporated into another document such as a health insurance enrollment form in accordance with Section R(3)(c), the signature need not appear on the same page as the language required under subsections (a), (b), and (c) above.

2. Level 2 Uses. Consent to Access or receive information via the SHIN-NY for the purposes of Level 2 Uses shall be obtained using a Level 2 Consent or an Alternative Consent approved by the Bronx RHIO under this Section R(2), which shall include (i) the information required pursuant to Section R(1) and (ii) the following information:

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

b. Whether the Bronx RHIO and/or its Participants will benefit financially as a result of the Disclosure of the patient's information;

c. The date or event upon which the patient's consent expires;

d. Acknowledgement that payers may not condition health plan enrollment and receipt of benefits on a patient's decision to grant or withhold consent;

e. A list of or reference to all Data Providers at the time of the patient's consent, as well as an acknowledgement that Data Providers may change over time and instructions for patients to access an up-to-date list of Data Providers through the Bronx RHIO website or other means; the consent form shall also identify whether the Bronx RHIO is party to data sharing agreements with other QEs and, if so, provide instructions for patients to access an up-to-date list of Data Providers from the Bronx RHIO website or by other means;

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

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

h. The date of execution of the consent.

3. Requirement for Separate Consents

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

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

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

4. Education Requirement for Level 2 Consents Relating to Marketing. When the Bronx RHIO or its Participant obtains a Level 2 Consent to Access or receive Protected Health Information via the SHIN-NY for the purpose of Marketing, the Bronx RHIO or its Participant must provide the patient with information about the nature of such Marketing.

5. Naming of QEs and Recognition of Consents.

   a. An Affirmative Consent form is not required to include the name of a QE.

   b. Up until a date to be determined by NYSDOH, a QE may continue to use an Affirmative Consent form on which the name of such QE appears.

   c. In the case where an Affirmative Consent form includes the name of at least one but not all QEs, a QE will Disclose to a Participant a patient's Protected Health Information even if such QE's name does not appear on the Affirmative Consent form so long as:

(1) the patient signed the Affirmative Consent form;

(2) the Affirmative Consent form indicates that the Participant is a potential recipient of the patient's Protected Health Information in accordance with Section R(1)(c); and

(3) the Disclosure otherwise complies with these Policies and Procedures.

S. Consents Covering Multiple Participants. In the event that the Bronx RHIO elects to use Affirmative Consents that apply to more than one Participant, the following conditions will apply:

1. The Participant offering the multi-Participant consent to the patient must inform the patient that the patient has an option to sign a consent form that applies only to that Participant.

2. If the multi-Participant consent allows a Participant to Access or receive any patient records that are subject to the rules governing federally-assisted alcohol or drug abuse programs at 42 C.F.R. Part 2, the consent form must comply with all relevant restrictions in 42 C.F.R. Part 2.

3. An Affirmative Consent may apply to Participants who join the Bronx RHIO after the date the patient signs the consent form, provided that: (i) the Bronx RHIO maintains a list of its Participants on the Bronx RHIO website and updates that list within 24 hours of when a new Participant is granted Access to patient information via the RHIO System; (ii) the Bronx RHIO mails a hard copy list of its Participants without charge to any patient who requests that list within 5 business days of the request; (iii) the consent form notifies patients that the list of Participants will be regularly updated on the Bronx RHIO website and that patients have the right to obtain a hard copy of the list, free of charge, upon request, and (iv) Access to any patient records that are subject to the rules governing federally-assisted alcohol or drug abuse programs complies with 42 C.F.R. Part 2.

T. Transmittals to Non-Participants

1. Transmittals to Business Associates. In any case where a Participant has a right to Access or receive Protected Health Information under these Policies and Procedures, the Participant may request that the Bronx RHIO Transmit such information to a Business Associate of the Participant, and the Bronx RHIO may comply with such request, so long as the conditions set forth in

subsections (a) through (f) are met. Nothing in this section shall allow the Bronx RHIO to treat a Business Associate as a Participant unless the Business Associate otherwise meets the definition of a Participant.

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

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

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

d. The Bronx RHIO reasonably believes that the Transmittal is in accordance with state and federal law and the terms of the Business Associate Agreement.

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

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

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

a. The patient has granted Affirmative Consent for the Transmittal, provided that Affirmative Consent shall not be required if the Transmittal is provided to a public health authority, as defined at 45 C.F.R. § 164.501. The Affirmative Consent shall meet all the requirements of a

Level 1 Consent or Alternative Consent, provided that if the recipient is a life or disability insurer that is not a governmental entity then the form shall have been approved by the applicable department(s) of insurance. For the avoidance of doubt, none of the exceptions to the Affirmative Consent requirement set forth in this Policy other than Section J of this Policy shall apply to Transmittals under this section.

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

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

(2) A Health Information Exchange Organization that does not operate in New York State.

(3) A public health authority, as defined at 45. C.F.R. § 164.501, that is not located in New York State.

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

(5) A disability insurer or life insurer that has (A) issued a disability or life insurance policy to the patient; (B) received an application from the patient for such a policy; or (C) received a claim for benefits from the patient.

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

d. The Bronx RHIO takes reasonable measures to authenticate that the recipient is the same individual or entity authorized in the patient's Affirmative Consent to receive the patient's Protected Health Information.

e. The Bronx RHIO enters into an agreement with the recipient that requires the recipient to:

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

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

(3) Notify the Bronx RHIO in writing and in the most expedient time possible if the recipient becomes aware of any actual or suspected Breach of Unsecured Protected Health Information;

(4) Represent that the recipient is not excluded, debarred, or otherwise ineligible from participating in any federal health care programs; and

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

f. Special requirements applicable to Transmittals to life or disability insurers. When the Bronx RHIO receives a query from a life or disability insurer seeking a patient's Protected Health Information, the Bronx RHIO shall send a confirmation to the applicable patient, via email or otherwise, that the patient has consented to share Protected Health Information with the life or disability insurer. If the patient objects to such disclosure, the Bronx RHIO shall not disclose the Protected Health Information to the life or disability insurer if such objection is received within two business days of the Bronx RHIO's notification of the patient. If the Bronx RHIO does not receive an objection from the patient within two business days, the Bronx RHIO may Transmit the patient's Protected Health Information to the life or disability insurer.

Nothing in this section shall be construed to prohibit a patient from Disclosing any of the patient's Protected Health Information the patient has received from the Bronx RHIO under Section III.B or III.C of Policy 1-13 to an individual or entity of the patient's choice.

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

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

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

1. The individual accessing or receiving ~~Participant~~ the Protected Health Information is a licensed physician or nurse practitioner whose professional responsibilities include determining the cause of death of a patient, or an individual acting under the supervision of such Practitioner~~other individual as may be authorized by the QE Privacy & Security Policies & Procedures to receive such information~~. Such ~~Practitioners~~ individuals may include Medical Examiners and Coroners who are licensed as physicians or nurse practitioners, or individuals acting under the supervision of such a Medical Examiner or Coroner.

2. The Bronx RHIO and the Participant abide by the minimum necessary standard set forth at Section III.E of Policy 1-4.

3. Protected Health Information originating from a facility subject to the New York Mental Hygiene Law is Disclosed only if the facility has requested that an investigation be conducted into the death of a

patient and the recipient is a Medical Examiner or Coroner that is licensed as physician or nurse practitioner.

X. Telehealth

1. Generally. Affirmative Consent shall not be required for the Bronx RHIO to disclose a patient's Protected Health Information to a Participant that provides telehealth services to such patient if:

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

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

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

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

   e. The Participant Accesses or receives the patient's Protected Health Information only during the time period specified in Paragraph 2, below.

2. Duration of telehealth verbal consent. The patient's verbal consent shall remain valid until the patient has an in-person encounter with the Participant or revokes consent, provided that the Participant:

   a. Informs the patient that the consent will persist until the patient has an in-person encounter with the Participant or revokes consent;

   b. Informs the patient of the patient's right to revoke consent by notifying the Participant of such revocation either verbally or in writing; and

c. Provides the patient with access to a written consent form that documents the terms of the verbal consent by either providing the patient with a copy of the form (via email, text, mail or otherwise) or an electronic link to such form.

3. The Participant shall keep a record of having provided such information to the patient. If the Participant fails to comply with requirements (a) through (c) above, the verbal consent shall remain valid only for 72 hours.

Y. Waivers During a Public Health Emergency. NYSDOH may waive provisions in this Policy and Procedure 1-3 and other provisions of these Policies and Procedures during a public health emergency under Section 319 of the Public Health Services Act if (i) the waiver assists QEs and/or their Participants in their response to the public health emergency; (ii) NYSDOH provides public notice of such waiver; and (iii) the waiver complies with applicable state and federal law

Bronx RHIO, Inc.
Policy and Procedure
1-4
Authorized Users, Access to and Uses of Data

Originally Adopted February 25, 2008
Amended and Restated as of December 15, 2014
Amended and Restated as of February 28, 2017
Amended and Restated as of September 25, 2017
Amended and Restated as of April 26, 2018
Amended and Restated as of June 27, 2019

I. Policy

It is the policy of the Bronx RHIO that Participants' Authorized Users must be authorized and trained in accordance with these Policies and Procedures in order to Access Protected Health Information through the RHIO System. Data may only be used for the purposes set forth in the applicable Affirmative Consent. Any other use of the data is a violation of these Policies and Procedures. Authorized Users may only Access and use Protected Health Information through the RHIO System in accordance with these Policies and Procedures.

II. Responsible Parties

Each Participant will be responsible for designating its Authorized Users and establishing the level of Access each Authorized User will have based, at a minimum, on the Authorized User's job function and relationship to patients of the Participant.

Participants utilizing a local authentication system (as opposed to the Bronx RHIO's central authentication system) will be responsible for designating an individual who will be responsible for activating each Authorized User's account in the Participant's local authentication system.

Participants utilizing the Bronx RHIO's central authentication system will be responsible for designating an individual who will be responsible for approving the application for each Authorized User's account and the Bronx RHIO will be responsible for entering information from the Authorized User Registration Form for such Participant's Authorized Users into the Bronx RHIO's central

authentication system and for activating those Authorized Users in the Bronx RHIO's central authentication system.

All Participants and the Bronx RHIO, as applicable, will be responsible for ensuring that Authorized Users only Access and use Protected Health Information through the RHIO System in accordance with these Policies and Procedures.

III. Procedure

A. Each Participant utilizing a local authentication system must establish a Policy for User Authorization, Access and Authentication that:

1. Determines who may Access clinical data through the RHIO System and the level of Access such individual may have based, at a minimum, on the individual's job function and relationship to the patient. Such Policy for User Authentication shall assign role-based Access rights in accordance with those set forth in Section A(13) below.

2. Assigns a unique user identifier to each Authorized User. Group or temporary user identifiers are prohibited.

3. Assigns a password to each Authorized User that meets the password strength requirements set forth in National Institute of Standards and Technology Special Publication 800-63, requires that the Authorized User change the password at least every 90 calendar days, and prohibits the Authorized User from reusing passwords.

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

5. Prohibits Authorized Users from sharing their identifiers, passwords or other authentication tools (e.g., tokens) with others, and directs Authorized Users to always use their own identifiers, passwords or other authentication tools to log into the RHIO System.

6. Provides that an Authorized User's right to Access clinical data through the RHIO System will be terminated upon termination of the Authorized User's employment with the Participant or upon

any violation by the Authorized User of these Policies and Procedures.

7. Provides that each Authorized User shall sign an acknowledgement that the Authorized User recognizes and understands the requirement to keep ~~his or her~~the Authorized User's identifier and password secret, and understands ~~his or her~~ the Authorized User's obligations under these Policies and Procedures, including but not limited to the Privacy Policy and Procedure.

8. Requires utilization of an authentication methodology that meets the minimum technical requirements for Authentication Assurance Level 2 set forth in National Institute of Standards and Technology Special Publication 800-63. If a Participant exceeds this requirement and authenticates its Authorized Users using multifactor authentication, which queries Authorized Users for something they know (e.g., a password) and something they have (e.g., an ID badge or a cryptographic key), then such Authorized Users are able to connect directly to the RHIO System. If a Participant does not authenticate its Authorized Users using multi-factor authentication, then such Authorized Users must utilize the Bronx RHIO's multi-factor authentication system. Participants that use multi-factor authentication may use a combination of tokens (authentication secrets to which an Authorized User's identity is bound), including soft cryptographic tokens with the key stored on a general-purpose computer, hard cryptographic tokens, which have the key stored on a special hardware device like a key FOB, or one-time password device tokens, which have a symmetric key stored on a personal hardware device (e.g., a cell phone) in a manner that protects against protocol threats, including eavesdropper, replay, online guessing, verifier impersonation, and man-in- the-middle attacks.

9. Provides that each Authorized User shall complete Training prior to activation of the Authorized User's access to the RHIO System and that each Authorized User shall undergo continuing and/or refresher training on an annual basis.

10. Requires the Participant to track when Authorized Users log in and log out and enforce a limit of five Failed Access Attempts by an Authorized User.

11. Requires the Participant to ensure that Authorized Users are automatically logged-out of the RHIO System after a period of inactivity specified in the Participant's Policy for User Authorization, Access, and Authentication.

12. Requires the Participant to ensure that each Authorized User complies with any other authentication requirements developed through the SCP.

13. Assigns one of the following roles to each of its Authorized Users:

    a. Authorized User with Break the Glass authority (limited to (i) Practitioners practicing in the Emergency Room, the Labor and Delivery Department, the Intensive Care Unit, and other Practitioners providing emergent care), (ii) Authorized User acting under the direction of a Practitioner and (iii) ~~Advanced~~ Emergency Medical Technician with Break the Glass authority.

    b. Practitioner with Access to clinical and non-clinical information.

    c. Non-Practitioner with Access to clinical and non-clinical information.

    d. Non-Practitioner with Access to non-clinical information. These individuals will have Access only to patient search and consent status screens in order to enter consents and/or demographic information into the RHIO System.

    e. Bronx RHIO administrators with Access to non-clinical information.

    f. Bronx RHIO administrators with Access to clinical information in order to engage in public health reporting in accordance with Section III.J of Policy 1-3 or other activities authorized under these Policies.

    g. Bronx RHIO administrators with Access to clinical and non-clinical information for the purpose of system maintenance and testing, trouble shooting and similar operational and technical support purposes.

    Prior to permitting any of its Authorized Users to Access the RHIO System, the Participant must provide a copy of such Policy for User Authorization, Access and Authentication to the Bronx RHIO and such Policy for User Authorization, Access and Authentication must be approved by the Executive Director of the Bronx RHIO.

B. Each Participant utilizing the Bronx RHIO's central authentication system must submit to the Bronx RHIO an Authorized User Registration Form for each of the individuals it wishes to activate as Authorized Users. Each

Participant shall notify the Bronx RHIO (i) of termination of an Authorized User's employment or affiliation with the Participant immediately or as promptly as reasonably practicable but in any event within one business day of termination and (ii) of a change in an Authorized User's role with the Participant that renders the Authorized User's continued access to the RHIO System inappropriate under the role-based Access standards as promptly as reasonably practicable.

C. When performing authorization, access and authentication activities on behalf of Participants using its central authentication system, the Bronx RHIO will comply with the requirements set forth at Sections A(1)-(13) above.

D. Each Participant must ensure the physical security of locations where Authorized Users access the RHIO System and compliance with privacy and security requirements of HIPAA and all other applicable confidentiality laws and regulations.

E. The Bronx RHIO and each Participant will make reasonable efforts, except in the case of Access for Treatment, to limit information Disclosed by the Bronx RHIO to the minimum amount necessary to accomplish the intended purpose for which it is being Disclosed.

F. During the process of identifying a patient and locating a patient's medical records through a Record Locator Service or other comparable directory, the Bronx RHIO and each Participant will (i) implement reasonable safeguards to minimize unauthorized incidental Disclosures of Protected Health Information, (ii) include the minimum amount of Demographic Information reasonably necessary to enable Authorized Users to successfully identify a patient through the Record Locator Service, and (iii) prohibit Authorized Users from Accessing Protected Health Information in any manner inconsistent with these Policies and Procedures and with the QE Privacy and Security Policies and Procedures.

G. Should the Bronx RHIO include Payer Organizations as Participants, it will ensure that a Payer Organization may not Access Protected Health Information through the RHIO System if a patient has requested, in accordance with the HIPAA Privacy Rule and HITECH, that the Participant creating such information not Disclose it to the Payer Organization.

H. Unless required by law or court order, the Bronx RHIO will not Disclose Protected Health Information to government agencies for health oversight purposes, such as Medicaid audits, professional licensing reviews, and fraud and abuse investigations.

I. The Bronx RHIO and its Participants shall identify individuals whose access to data may bypass or enable circumvention of activity logging, access controls, or other security controls. These Authorized Users shall be subject to heightened scrutiny both in hiring and in ongoing auditing and monitoring of their activities. Such heightened scrutiny may include pre-employment (or pre-engagement for contractors) background checks; mandatory privacy and security training and annual retraining; a formal termination procedure more stringent and timely than that set forth for other Authorized Users; regular review of access privileges, user accounts; or other measures as the Bronx RHIO or Participant may deem appropriate given their security risk assessment.

J. Certified Applications.

1. In the event that the Bronx RHIO permits Access to the RHIO System by Participants through one or more Certified Applications, the Bronx RHIO will implement systems consistent with the SHIN-NY Policy Guidance for authenticating each Certified Application's credentials in connection with each Access request.

2. Each Participant Accessing Protected Health Information through a Certified Application shall authenticate the Participant's users in a manner consistent with these Policies and Procedures.

3. Participant using a Certified Application shall provide the Bronx RHIO 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~~such individual is personally responsible for the use of the Certified Application for this purpose. The Participant shall update this information and provide a new certification prior to changing the individual responsible for the use of the Certified Application.

4. Each Participant using a Certified Application shall limit Access to any Protected Health Information obtained through the Certified Application to individual users of the Participant's information system who would be eligible to be Authorized Users of the Participant under these Policies and Procedures if they were Accessing Protected Health Information directly through the Bronx RHIO. Each Participant shall credential, train and otherwise manage the Access of such users to Protected Health Information obtained through the Bronx RHIO in accordance with the provisions of this Section 4 applicable to Authorized Users.

Bronx RHIO, Inc.
Policy and Procedure
1-5
Training

Originally Adopted February 25, 2008
Amended and Restated as of December 15, 2014
Amended and Restated as of February 28, 2017
Amended and Restated as of June 27, 2019

I. Policy

It is the policy of the Bronx RHIO to assure that in building and operating the RHIO System the focus is maintained on the welfare, safety and concerns of the patient. For this reason it is important that all users be very aware of the privacy and confidentiality concerns of patients and be thoroughly trained in the appropriate use of the RHIO System.

Accordingly:

- It is the policy of the Bronx RHIO to allow only individuals who are trained and certified through the Bronx RHIO training program to qualify as Authorized Users and Access clinical data through the RHIO System;

- It is the policy of the Bronx RHIO to allow only individuals who are trained and certified through the Bronx RHIO training program to qualify as Authorized Users for the limited purpose of entering consents and/or demographic information into the RHIO System; and

- It is the policy of the Bronx RHIO to allow only individuals who are trained and certified through the Bronx RHIO training program to collect and record patients' Affirmative Consent.

II. Responsible Parties

The Bronx RHIO will be responsible for developing and maintaining training programs for: (i) Authorized Users; and (ii) those who collect and record patients' Affirmative Consent. The Bronx RHIO will be responsible for determining the modality of the training programs, e.g., online tutorial, "face-to-face" training to designated individuals at each site, or train-the-trainer. Such

training may be tailored to reflect the purposes for which an Authorized User is authorized to Access Protected Health Information through the RHIO System as well as the nature and scope of the Protected Health Information Accessed.

Each Participant will be responsible for coordinating the training of designated individuals to become Authorized Users and/or to collect consent forms, and if a train-the-trainer model is used, each Participant will be responsible for designating the trainer(s) at the site to be trained by the Bronx RHIO, and for implementing the training.

Each Participant will be responsible for assuring that all individuals that wish to become Authorized Users and/or to collect consent forms have met the Bronx RHIO's standard that defines when learners have mastered the material and can demonstrate the ability to perform the training objectives. The standard will be distributed along with the training materials.

Each Participant will be responsible for designating a Training Program Administrator to be responsible for the registration, tracking and results reporting processes for their respective sites, in coordination with the Bronx RHIO office.

The Bronx RHIO will be responsible for training and supporting the Participants' Training Program Administrators in performing their roles.

III. Procedure

A. Training and Certification of Authorized Users.

The Bronx RHIO will deploy a face to face or Online Training Program for individuals who wish to become Authorized Users and Access clinical information through the RHIO System.

B. Training and Certification of Personnel Who Collect and Record Patients' Affirmative Consent.

The Bronx RHIO will deploy a face to face or Online Training Program for Participant personnel who wish to collect and record patients' Affirmative Consent. Such Training Program may be combined with the Training Program for Authorized Users described in Section III (A).

C. Implementation of Online Training Programs.

In implementing any face to face or Online Training Programs, the Bronx RHIO will:

1. Determine the schedule for implementing the programs and announce the program and implementation schedule to the Participants;

2. Inform Participants on how the programs will work, who should be trained and how to use the decentralized administration software for scheduling and managing training;

3. Where applicable, train each Participants' Training Program Administrator, whose role is to:

    a. Ensure that individuals who wish to become Authorized Users and/or to collect consent forms participate in the programs;

    b. Track who passes the tests included as part of the programs and receives certification to become an Authorized User and/or to collect and record patients' Affirmative Consent.

    c. Provide reports to the Bronx RHIO identifying who completed the training programs, passed the tests and received certification;

    d. For Participants utilizing a local authentication system, arrange for activation of the accounts of Authorized Users who have completed the necessary training programs, passed the tests, and received necessary certifications in the Participant's local authentication system;

    e. Ensure that each Authorized User undergoes refresher training on an annual basis (or as needed based on any policy or procedure change) and maintain records of such training for audit for a period of at least six years; and

    f. Provide reports to the Bronx RHIO identifying who completed the annual refresher or as needed training programs.

4. Review and finalize the training program content.

5. Conduct user acceptance testing of the program.

6. Implement and monitor the program.

7. Coordinate with and support each Participant's Training Program Administrator to address and resolve administrative issues that may arise.

D. Appointment of Training Program Administrators.

1. Each Participant shall assign one individual to perform the role of Training Program Administrator as described in procedure C.3 above.

E. Other Responsibilities of the Bronx RHIO

1. The Bronx RHIO shall periodically review the Online Training Programs for quality and implement corrections and improvements as needed.

2. The Bronx RHIO shall provide ongoing training to train existing Authorized Users on upgrades and enhancements to the RHIO System resulting from new releases of software and the availability of new types of data.

3. The Bronx RHIO shall perform self-audits that ensure that if training is delegated to Participants, the Bronx RHIO regularly collects attestations by Participants that specifies for which of their Authorized Users annual refresher training has occurred. If training is completed by the Bronx RHIO, the Bronx RHIO shall be able to attest for which of its Participants and/or Authorized Users annual refresher training has occurred

Bronx RHIO, Inc.
Policy and Procedure
1-6
System and Data Security

Originally Adopted February 25, 2008
Amended and Restated as of June 30, 2014
Amended and Restated as of April 26, 2018

I. Policy

It is the policy of the Bronx RHIO that appropriate physical security will be maintained by the Bronx RHIO and the Participants for all hardware used in connection with the RHIO System. It is the policy of the Bronx RHIO to store all Protected Health Information in the United States.

II. Responsible Parties

Participants will have responsibility for maintaining the security of the workstations through which their Authorized Users access the RHIO System.

The Executive Director of the Bronx RHIO will have responsibility for maintaining the security of the hardware, if any, located at the Bronx RHIO's offices and used in connection with the RHIO System.

The Executive Director of the Bronx RHIO will have responsibility for ensuring that its technology vendor maintains the security of the hardware located in the technology vendor's data center (the "Data Center").

The Executive Director of the Bronx RHIO will have responsibility for ensuring that the Bronx RHIO and its technology vendor store all Protected Health Information in the United States.

III. Procedure

A. Participants are expected to comply with all applicable laws and regulations regarding system security, including, meeting the standards established by HIPAA pertaining to system security and workstation security.

B. The Bronx RHIO will comply with all applicable laws and regulations regarding system security, including (a) meeting the standards established by HIPAA pertaining to system security and workstation security, if applicable and (b) complying with the provisions of Section D below with respect to the hardware, if any, located at the Bronx RHIO's offices and used in connection with the RHIO System.

C. The Bronx RHIO will ensure that its technology vendor complies with all applicable laws and regulations regarding system security, including, at a minimum (a) meeting the standards established by HIPAA pertaining to system security and workstation security, if applicable and (b) complying with the provisions of Section D below with respect to Bronx RHIO hardware located in the Data Center.

D. The Bronx RHIO and the Participants will comply with, and the Bronx RHIO will ensure that its technology vendor complies with, the following system security standards:

1. To protect the confidentiality, integrity and availability of the RHIO System by taking reasonable steps to protect the RHIO System hardware, as well as the facilities in which it is located, from unauthorized physical access, tampering and theft.

2. To physically locate RHIO System hardware in locations where physical access can be controlled in order to minimize the risk of unauthorized access.

3. To take reasonable steps to ensure that the perimeter of facilities containing RHIO System hardware is physically sound, the external walls are properly constructed and the external doors have the appropriate protections against unauthorized access.

4. To prevent against unauthorized access to the facilities at which RHIO System hardware is located by ensuring that doors and windows of all facilities are locked when unattended and that external protections, such as window guards or bars, are installed on all windows at ground level and any other windows as reasonably necessary to prevent unauthorized entry.

5. To establish and document detailed rules to determine which workforce members are granted physical access rights to specific areas where the RHIO System is maintained and to provide such physical access rights to the work area only to workforce members having a need for access to such an area in order to complete job responsibilities.

6. To store all Protected Health Information in the United States.

E. In addition, the Bronx RHIO will ensure that its technology vendor complies with the following system security standards with respect to the Data Center:

1. To use the following controls at all delivery and loading areas to prevent unauthorized access to its facilities:

    a. Restrict access to a holding area from outside the building to identified and authorized workforce members.

    b. Design the holding area so supplies can be unloaded without delivery staff gaining access to other areas of the building.

    c. Secure the external doors of the holding area when the internal door of the area is open.

2. To take reasonable steps to ensure that the level of protection provided for the RHIO System, as well as the facilities in which they are housed, is commensurate with that of the identified threats and risks to the security of the RHIO System and its facilities. The technology vendor shall perform a periodic risk analysis in order to assess the level of physical access risk and adjust procedures accordingly.

Bronx RHIO, Inc.
Policy and Procedure
1-7
Audit Policy and Procedure

Originally Adopted February 25, 2008
Amended and Restated as of June 30, 2014
Amended and Restated as of February 28, 2017
Amended and Restated as of September 25, 2017
Amended and Restated as of April 26, 2018
Amended and Restated as of June 27, 2019

I. Policy

It is the policy of the Bronx RHIO to require that all Participants participate in audits on a regular basis in order to ensure that the RHIO System is being used only for purposes authorized by the Participation Agreement and these Policies and Procedures, and that each individual who views the data through the RHIO System is doing so in a manner consistent with the Participation Agreement and these Policies and Procedures, including but not limited to the Privacy Policy and Procedure. In addition, it is the policy of the Bronx RHIO to require that all Participants cooperate with the Bronx RHIO and/or other Participants with respect to any audits.

II. Responsible Parties

A. The Patient Rights and Member Responsibilities Committee of the Bronx RHIO is responsible for recommending to the Board of Directors the audits to be performed, the specific controls to be audited and the frequency and sample size for each audit. The Patient Rights and Member Responsibilities Committee is also responsible for reviewing the results of the audits and any corrective action to be taken as a result of problems uncovered during the audits. The Patient Rights and Member Responsibilities Committee will make recommendations to the Board of Directors as to whether the specified corrective action should be accepted.

B. The RHIO staff is responsible for assembling the list of cases to be sampled for each audit, for maintaining the audit schedule, for notifying

Participants when audits are due and for keeping the Patient Rights and Member Responsibilities Committee informed of all audit activity.

C. The Participants are responsible for carrying out audits on the sample of cases given to them by the RHIO staff in accordance with this Audit Policy and Procedure. In addition, each Participant is responsible for reviewing the results of its audits and determining whether corrective action is necessary, and reporting such results and any required corrective action plans to the Patient Rights and Member Responsibilities Committee.

D. The Participants are responsible for providing patients with information about who Accessed or received their Protected Health Information, in accordance with these Policies and Procedures and the QE Privacy & Security Policies & Procedures.

E. The RHIO staff is responsible for providing Participants with information about who Accessed or received their patients' information, including information to enable Participants to respond to patient requests for such information, in accordance with these Policies and Procedures and the QE Privacy and Security Policies and Procedures.

III. Procedure

A. The Bronx RHIO will maintain, for a period of at least six years from the date on which the information is Disclosed, immutable Audit Logs that document all Disclosures of Protected Health Information through the RHIO System.

1. Audit Logs will include, at a minimum, the following information regarding each instance of Access to Protected Health Information through the RHIO System:

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

b. The identity of the Authorized User Accessing the Protected Health Information;

c. The identity of the Participant with which such Authorized User is affiliated;

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

e. The date and time of Access;

f. The source of the Protected Health Information (i.e., the identity of the Participant from whose records the Accessed Protected Health Information was derived);

g. Unsuccessful Access (log-in) attempts; and

h. Whether Access occurred through a Break the Glass incident.

2. Audit Logs will include, at a minimum, the following information regarding each Transmittal of Protected Health Information through the RHIO System:

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

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

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

d. The date and time of Transmittal;

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

3. Other Requirements with Respect to Audit Logs and Access

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

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

4. Other Requirements with Respect to Audit Logs and Transmittals

a. The Bronx RHIO shall not be required to include a Transmittal within an Audit Log in cases where the Bronx

RHIO Transmits Protected Health Information from one Participant to another Participant, or to a Business Associate of another Participant, in accordance with written instructions from the recipient and without modification to the data being Transmitted (as may occur in the case of a One-to-One Exchange).

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

B. At least on an annual basis, or more frequently as may be determined by the Patient Rights and Member Responsibilities Committee, the Bronx RHIO will generate a random sample of records to be audited and the Participant will be responsible for auditing such records to establish the following with respect to each such record:

1. That an Affirmative Consent is on file for each patient for whom the Participant's Authorized Users Accessed Protected Health Information through the RHIO System.

2. That any Authorized User who Accessed Protected Health Information of a patient did so for a purpose authorized by the Affirmative Consent signed by the patient.

3. That a minor's Protected Health Information was Accessed without the Affirmative Consent of the minor's parent or guardian only in accordance with Section 1-3(III)(D) of these Policies and Procedures.

4. That clinical data was Accessed without Affirmative Consent by Authorized Users through the "Break the Glass" function only in accordance with Section 1-3(III)(E) of these Policies and Procedures.

5. Such other audits that may be recommended by the Patient Rights and Member Responsibilities Committee and approved by the Board of Directors.

C. If a Participant Accesses Protected Health Information through a Certified Application, the audits described in Section B shall include Access by the Participant's users through the Participant's system.

D. Audits will be conducted on a statistically significant sample size. The Patient Rights and Member Responsibilities Committee will consult technical experts as necessary to determine appropriate sample sizes for the audits set forth above.

E. The Patient Rights and Member Responsibilities Committee will meet at least quarterly to determine whether any additional audits need to be performed and to review the results of completed audits.

F. Notwithstanding the foregoing, all Break the Glass incidents shall be audited.

G. Each Participant will carry out the audits required by this Audit Policy and Procedure, as well as any additional audits that may be recommended by the Patient Rights and Member Responsibilities Committee and approved by the Board of Directors. Such audits will be performed in accordance with the schedule of audits recommended by the Patient Rights and Member Responsibilities Committee and approved by the Board of Directors. Each Participant will report the result of all such audits to the Patient Rights and Member Responsibilities Committee in the format specified by the Patient Rights and Member Responsibilities Committee. If any audit identifies any non-compliance with the Participation Agreement or any of these Policies and Procedures, the Participant will submit a corrective action plan to the Patient Rights and Member Responsibilities Committee along with the audit report.

H. The Patient Rights and Member Responsibilities Committee will review the audit reports and any corrective action plans, and will report to the Board of Directors any findings of non-compliance. With respect to each corrective action plan, the Patient Rights and Member Responsibilities Committee shall recommend to the Board of Directors whether the corrective action plan be accepted as presented, be revised as per agreement reached at the Patient Rights and Member Responsibilities Committee meeting or be rejected. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Board may vote to suspend access to the RHIO System for either the Participant or one or more Authorized Users of such Participant until the problem is adequately addressed.

I. The Bronx RHIO will provide Participants, upon request and as promptly as reasonably practicable but in no event more than 10 calendar days after the receipt of such request, the following information regarding any patient of the Participant whose Protected Health Information was Disclosed via the RHIO System, provided the patient has provided such Participant with Affirmative Consent to Access ~~his or her~~the patient's Protected Health Information through the RHIO System:

1. The name of each Authorized User who Accessed such patient's Protected Health Information in the prior 6-year period;

2. The Participant through which such Authorized User Accessed such Protected Health Information;

3. The time and date of Disclosure; and

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

J. Patient Access to Audit Information

1. Subject to laws granting minors the right to keep Minor Consent Information confidential from their parents or guardians, each Participant will provide patients, upon request, with the following information:

   a. The name of each Participant who Accessed or received the patient's Protected Health Information in the prior 6-year period;

   b. The time and date of the Disclosure; and

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

2. If a patient requests the name(s) of the Authorized User(s) who Accessed ~~his or her~~the patient's Protected Health Information through a specific Participant in up to the prior 6-year period, the Bronx RHIO and that Participant shall take the following actions:

   a. The Bronx RHIO will inform the Participant of the request and will provide the Participant with the list of the Participant's Authorized User(s) who Accessed the patient's Protected Health Information through the RHIO System in up to the prior 6-year period.

   b. The Participant shall either provide the list of Authorized User(s) to the patient or undertake an audit to determine if

the Authorized User(s) on the list appropriately Accessed the patient's Protected Health Information for Authorized Purposes.

c. If the Participant chooses to undertake an audit of its Authorized User Access and determines that all of the Authorized User(s) Accessed the patient's information for Authorized Purposes, the Participant shall inform the patient of this finding and need not provide the patient with the names of the Authorized User(s) who Accessed that patient's information.

d. If the Participant chooses to undertake an audit of its Authorized User Access and determines that one or more of the Authorized User(s) did not Access the patient's information for Authorized Purposes, the Participant shall, subject to laws granting minors the right to keep Minor Consent Information confidential from their parents or guardians, (i) inform the patient of this finding; (ii) provide the patient with the name(s) of the Authorized User(s) who inappropriately Accessed the patient's information unless the Participant has a reasonable belief that such disclosure could put the Authorized User at risk of harm, in which case the Participant shall provide the patient with an opportunity to appeal this determination to a representative who is more senior to the individual(s) who made the original determination; and (iii) inform the Bronx RHIO of the inappropriate Access and otherwise comply with the requirements of this Section III.J.2.

3. Each Participant will provide the information in this Section J as promptly as reasonably practicable but in no event more than ten calendar days after receipt of the request.

4. Each Participant will provide the information in this Section J to patients at no cost once in every 12-month period and may charge patients a fee, as approved by the Board of Directors, for any additional requests within a given 12-month period. Each Participant will waive such fee where such additional request is based on a patient's allegation of unauthorized Access to the patient's Protected Health Information through the RHIO System.

K. The Bronx RHIO will make the results of certain of the periodic audits conducted by its Participants available on its website as promptly as reasonably practicable, but not more than 30 days after completion of the audit.

L. In the most expedient time possible, the Bronx RHIO, with the assistance of its Participants, shall investigate the scope and magnitude of any data inconsistency or potential error that was made in the course of the Bronx RHIO's data aggregation and exchange activities and, if an error is determined to exist, identify the root cause of the error and ensure its correction. The Bronx RHIO shall log all such errors, the actions taken to address them and the final resolution of the error. The Bronx RHIO shall also make reasonable efforts to identify Participants that Accessed or received such erroneous information and to notify them of corrections. This provision does not apply to updates to data that are made by Data Providers in the ordinary course of their clinical activities nor does it apply to updates to Demographic Information.

M. Weekly Audit Reports by Organ Procurement Organizations. Organ Procurement Organizations shall provide weekly confirmation that all instances in which Protected Health Information was Accessed through the RHIO System by the Organ Procurement Organization's Authorized Users were consistent with the terms of these Policies and Procedures (based upon a listing sent by the Bronx RHIO).

N. Additional Requirements Related to Auditing of Public Health Access. The Bronx RHIO shall use special safeguards with respect to audits of Access by Public Health Agencies, which shall include at least the following:

1. The Bronx RHIO shall create, on a regular basis, an audit report of Authorized User activity for each Public Health Agency workgroup that will include, at a minimum, the patient names, times, dates and reason for access for each Authorized User.

2. The name of the particular Public Health Agency shall be listed in the patient Audit Logs.

3. The Bronx RHIO shall follow-up with workgroup manager(s) if approval of an audit report is not received. If the attempt to contact the workgroup manager(s) is unsuccessful, the Bronx RHIO may suspend all Authorized User accounts associated with that particular workgroup until the situation is resolved.

Bronx RHIO, Inc.
Policy and Procedure
1-8
Breach Response

Originally Adopted February 25, 2008
Amended and Restated as of June 30, 2014

I. Policy

It is the policy of the Bronx RHIO that Participants be responsible for immediately investigating and mitigating to the extent possible, any Breach that they become aware of, and for reporting the Breach to the Executive Director of the Bronx RHIO for any needed investigation or mitigation. It is also the policy of the Bronx RHIO that the Bronx RHIO be responsible for reporting any Breach the Bronx RHIO becomes aware of to any Participants affected by such Breach, and for assisting Participants in the investigation and mitigation of any such Breach. In addition, it is the policy of the Bronx RHIO that Participants be responsible for notification of individuals affected in accordance with applicable federal, state and local laws and regulations, including but not limited to HITECH, the New York State Information Security Breach Notification Act (New York General Business Law § 899-aa), and HIPAA, with the assistance, if necessary, of the Bronx RHIO if the Breach involves more than one Participant. Finally, it is the policy of the Bronx RHIO that Participants and the Bronx RHIO cooperate with each other in the investigation and mitigation of any Breach that they become aware of.

II. Responsible Parties

Each Participant is responsible for investigation, mitigation and reporting of any actual or potential Breach that such Participant becomes aware of relating to the RHIO System, and for cooperating with the Bronx RHIO and the other Participants in the investigation and mitigation of any actual or potential Breach involving the Participant.

The Executive Director of the Bronx RHIO is responsible for reporting any actual or potential Breach the Executive Director becomes aware of to any Participants that may be affected by such Breach, for assisting Participants in the investigation and mitigation of any Breach, and for coordinating the investigation and

mitigation of any actual or potential Breach that involves more than one Participant.

III. Procedure

A. In the event that a Participant becomes aware of a suspected or actual Breach, the Participant shall immediately:

1. Investigate the scope and magnitude of the Breach.

2. Identify the root cause of the Breach

3. Mitigate the Breach to the extent possible.

4. Notify the Executive Director of the Bronx RHIO in writing of the Breach and cooperate with the Executive Director and the RHIO Staff on any investigation of the potential impact of the Breach on the Bronx RHIO and any other Participants.

5. In the event that the Breach involves or may involve more than one Participant, cooperate with the Bronx RHIO and the other Participant(s) in investigating and mitigating the Breach, including but not limited to sharing any information that may be necessary in connection with such investigation and/or mitigation, subject to all applicable laws and regulations.

6. Notify regulatory agencies and customers in compliance with all applicable state and federal laws, rules, and regulations.

7. If the breach is covered under either HITECH or the New York State Information Security Breach Notification Act, meet with the Bronx RHIO and all affected entities to develop a plan for the response. Each response will be different according to the situation.

B. In the event that the Executive Director becomes aware of a suspected Breach, the Executive Director shall determine whether an actual Breach has occurred and, if so, identify the root cause. The Executive Director shall then:

1. Report any Breach to any Participants that may be affected by such Breach.

2. Assist the Participants in the investigation and mitigation of any Breach, including but not limited to sharing any information that may be necessary in connection with such investigation and/or mitigation, subject to all applicable laws and regulations.

3. Coordinate the investigation and mitigation of the Breach should it involve more than one Participant.

4. Assure that all proper notifications have been made by the entities involved.

5. Provide a report of any Breach and mitigation actions taken to the Board of Directors.

6. Impose on Participants any such sanctions as may be recommended by the Board of Directors.

Bronx RHIO, Inc.
Policy and Procedure
1-9
Member Responsibility for System Support

Originally Adopted February 25, 2008
Amended and Restated as of December 15, 2014

I. Policy

It is the policy of the Bronx RHIO that each Participant is responsible for maintaining internet connectivity and providing such other system support services as may be necessary for ongoing operation of the RHIO System in such Participant's facility, and for cooperating with the Bronx RHIO and its vendors in maximizing the utility and effectiveness of the RHIO System for such Participant's Authorized Users.

II. Responsible Parties

Each Participant will be responsible for providing the system support services necessary for activities related to viewing data using the RHIO System.

Data Providers will also be responsible for the obligations set out at Section III (B) below.

III. Procedure

A. Each Participant is responsible for:

1. Maintaining internet connectivity and for the performance of the RHIO System as limited by that connectivity.

2. Working with the Bronx RHIO to develop and implement methods to enable Authorized Users to access the RHIO System, such as providing an icon to enable easy access to the RHIO System on each workstation that accesses the RHIO System or a single-sign on process from the Participant's electronic medical record. Participant shall ensure that the RHIO System remains accessible through such method.

3. Providing the first level of support to its Authorized Users by, at a minimum, taking calls and documenting issues relating to access to and performance of the RHIO System that can then be escalated, if necessary, to the Bronx RHIO's Help Desk.

4. Cooperating with the Bronx RHIO's support personnel in troubleshooting any difficulties experienced by Authorized Users with respect to access to and performance of the RHIO System.

5. Cooperating with the Bronx RHIO and its vendors in testing and implementing upgrades to the RHIO System.

B. A Data Provider is further responsible for:

1. Monitoring data feeds from its legacy systems to the RHIO System and solving any problems that may arise with respect to such data feeds, ensuring accurate and complete loading of clinical data from its legacy systems to the RHIO System.

2. Notifying the Bronx RHIO of any problems in the regular feeds of data to the RHIO System.

3. Ensuring that appropriate Change Management processes are in place so that the impact on the RHIO System of any changes to the legacy systems or operating environment are evaluated and tested, as necessary.

4. Notifying the Bronx RHIO of system changes that will require an update to the RHIO System so that the Bronx RHIO can participate in modification and/or testing procedures.

5. Monitoring connectivity to the RHIO System and coordinating with RHIO support services in accordance with the escalation process developed by the Bronx RHIO as necessary to troubleshoot and resolve any problems or issues.

6. Following documented procedures provided by the Bronx RHIO for escalation of any problem or issue that may arise with the use or maintenance of the RHIO System that cannot be resolved locally.

7. Performing periodic data integration audits to determine whether data in the RHIO System accurately reflects current data from the legacy system, in accordance with requirements established by the Patient Rights and Member Responsibilities Committee and approved by majority vote of the Board of Directors.

8. Cooperating with the Bronx RHIO to investigate and resolve any issue identified by the Bronx RHIO and communicated to the Participant.

Bronx RHIO, Inc.
Policy and Procedure
1-11
Insurance

Originally Adopted February 25, 2008
Amended and Restated as of June 30, 2014

I. Policy

It is the policy of the Bronx RHIO that the Bronx RHIO and each of the Participants maintain such insurance coverage as is reasonable and necessary with respect to its use of the RHIO System and its obligations under the Participation Agreement.

II. Responsible Parties

The Bronx RHIO will have responsibility for obtaining insurance coverage for the Bronx RHIO in accordance with the requirements of this policy.

Each of the Participants will have responsibility for obtaining insurance coverage for such Participant in accordance with the requirements of this policy.

III. Procedure

A. The Bronx RHIO shall obtain and maintain insurance in the minimum amount required for QEs under the SHIN-NY Policy Guidance.

B. Each Participant shall obtain and maintain the following insurance coverage:

1. Professional liability insurance coverage in the minimum amounts of one million dollars per claim and three million dollars in the aggregate. In lieu of this insurance coverage, a Participant may provide evidence of Federal Tort Claims Act coverage of the Participants and its physicians and other professional staff.

2. Comprehensive general liability insurance coverage in the minimum amount of one million dollars per occurrence and three million dollars in the aggregate.

C. In the event that a Participant obtains any of the insurance coverage required by this policy on a "claims made" or similar basis, such Participant shall, in the event of termination of Participant's participation in the Bronx RHIO, obtain and maintain a tail policy providing equivalent coverage for a period of at least three years after such termination.

D. All insurance coverage required by this policy shall be provided under valid and enforceable policies issued by insurance companies legally authorized to do business in the State of New York.

E. Upon request of the Bronx RHIO, Participants shall provide the Bronx RHIO with certificates of insurance evidencing such coverage.

F. In lieu of obtaining the insurance coverage required in this policy, a Participant may, subject to the approval of the Board of Directors, self-insure its professional liability or its commercial general liability. Participant shall maintain a separate reserve for its self-insurance. If a Participant will use the self-insurance option described in this paragraph, the Participant will provide to the Bronx RHIO a statement verified by an independent auditor or actuary that its reserve funding levels and process of funding appears adequate to meet the requirements of this section and fairly represents the financial condition of the fund. The Participant will provide a similar statement during the term of this Agreement upon the Bronx RHIO's request, which will be made no more frequently than annually. The Participant will assure that its self-insurance fund will comply with applicable laws and regulations.

G. Notwithstanding the foregoing, each of the New York City Health and Hospitals Corporation and the New York City Department of Health and Mental Hygiene shall be exempt from obtaining the insurance coverage required in this policy based upon its representation that it shall be responsible for its acts or omissions and the acts or omissions of its constituent facilities in connection with the Participation Agreement, which representation is based upon and limited to the obligation of the City of New York to defend, indemnify and hold harmless its officers, employees, agents and contracted affiliates from any and all liability and damages arising from or in connection with the provision and delivery of health services.

Bronx RHIO, Inc.
Policy and Procedure
1-12
Participant Termination

Originally Adopted February 25, 2008
Amended and Restated as of June 30, 2014
Amended and Restated as of June 27, 2019

I. Policy

It is the policy of the Bronx RHIO that upon termination of a Participant's participation in the Bronx RHIO, whether such termination is initiated by the Participant or by the Bronx RHIO, the Participant and the Bronx RHIO shall cooperate to ensure that patient data from the terminating Participant is no longer Disclosed via the RHIO System as of the termination date, that all relevant data is preserved to ensure the Bronx RHIO's ability to respond, or to assist Participants in responding, to any audits, investigations, claims, suits or other legal or patient queries relating to patient data provided or Accessed or received by the terminating Participant through the RHIO System prior to such termination, and that any RHIO assets (i.e., hardware) are properly protected.

II. Responsible Parties

The Board of Directors will have primary responsibility for overseeing the execution of this termination policy.

The Executive Director will oversee the activities of the Bronx RHIO and its agents to complete the tasks defined in this policy and enforce its terms.

The Participants will have responsibility for ensuring compliance with this policy at their sites.

III. Procedure

A. For Data Providers:

1. As of the effective date of termination of a Participant's Participation Agreement, the Bronx RHIO's technology vendor will block Disclosure of any data made available by the Participant

through the RHIO System, and will provide the Participant with a certification that such actions have been taken.

2. The Bronx RHIO shall have the right to maintain access to any data made available by the Participant to the RHIO System for such period of time as may be determined by majority vote of the Board of Directors, in a manner that ensures the data will be available as needed to allow the Bronx RHIO and/or the other Participants, as the case may be, to respond to any audits, investigations, claims, suits or other legal or patient queries relating to patient data provided or Accessed or received by the terminating Participant through the RHIO System prior to such termination.

3. The Bronx RHIO will update its website and other materials in a timely manner to remove the name of the terminating Participant, and will notify all other Participants that the terminating Participant has terminated its participation in the Bronx RHIO, and the effective date of such termination.

4. The Participant will pay for the out-of-pocket expenses incurred by the Bronx RHIO in conjunction with the termination.

Bronx RHIO, Inc.
Policy and Procedure
1-13
Patient Education, Engagement and Access

Adopted June 30, 2014
Amended and Restated as of February 28, 2017
Amended and Restated as of September 25, 2017
Amended and Restated as of April 26, 2018
Amended and Restated as of June 27, 2019
Amended and Restated as of April 29, 2021
Amended and Restated as of October __, 2021

I. Policy

It is the policy of the Bronx RHIO to educate patients and/or their Personal Representatives about how their Protected Health Information will be Disclosed through the RHIO System, including the process of providing Affirmative Consent, about their rights to access their Protected Health Information through the RHIO System, including whether such access is available, about the RHIO's Data Providers, and to assure meaningful patient/consumer input and participation into its operations and decision-making.

II. Responsible Parties

The Executive Director will ensure the Bronx RHIO's compliance with this policy.

The Participants will have responsibility for educating patients and/or their Personal Representatives about their rights, if any, to access their Protected Health Information through the RHIO System, including informing them of whether such access is available.

III. Procedure

A. The Bronx RHIO will educate patients and/or their Personal Representatives about the process and risks and benefits of providing Affirmative Consent and the terms and conditions upon which their Protected Health Information will be Disclosed~~, and will conform its~~

1776 Eastchester Rd., Suite 200, Bronx, NY 10461
Phone 718-708-6630 Fax 718-708-7272

~~patient education activities to any patient education program standards developed through the Statewide Collaboration Process~~.

B. The Bronx RHIO will facilitate the access of patients and their Personal Representatives to the patients' Protected Health Information maintained by the Bronx RHIO through one of the following mechanisms: (a) through its own web-based portal or through Participants' web-based portals; (b) through a web-based portal established by or maintained by a third party on behalf of a patient, including a Patient App, provided that the requirements related to disclosures to third parties set forth in Section C below are met; (c) by providing a paper or electronic copy of information maintained about the patient by the Bronx RHIO or (d) through any other mechanism requested by the patient (provided that the Bronx RHIO need not provide the Protected Health Information via the requested mechanism if applicable law, including the Information Blocking Rules, permit the Bronx RHIO to use an alternative mechanism. Each patient has the right to indicate the scope of the Protected Health Information and which of these mechanisms offered ~~he or she~~ the patient prefers to utilize to obtain access to ~~his or her~~ the patient's information, and the Bronx RHIO will abide by the patient's request unless applicable law (including the patient access provisions under the HIPAA Privacy Rule or the requirement for the "content and manner" Exception or another Exception to the Information Blocking Rules) permit or require the Bronx RHIO to limit the scope and form of the Protected Health Information provided to the patient. The Bronx RHIO will only facilitate such access after confirming the identity of the patient or the patient's Personal Representative through adequate identity proofing procedures.

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

1. The Bronx RHIO will Disclose the patient's Protected Health Information in response to the patient's or Personal Representative's request only after confirming the identity of the patient or the patient's Personal Representative that submitted the request through adequate identity proofing procedures. For example, the Bronx RHIO may require patients to provide their demographic information in conjunction with an image of their government-issued photo ID.

2. The Bronx RHIO may decline to fulfill the request, or fulfill the request only in part, only if applicable law permits the Bronx

RHIO to do so or if the patient or the patient's Personal Representative withdraws the request. Applicable law may include, but is not limited to, the patient access provisions under the HIPAA Privacy Rule, the Information Blocking Rules, or state laws that limit disclosures to Patient Apps.

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

4. The Bronx RHIO will require a patient, a patient's Personal Representative, or a third party to pay a fee prior to Disclosing Protected Health Information to a third party only if applicable law, including the patient access provisions under the HIPAA Privacy Rule and the Information Blocking Rules, permit such fee to be charged. For example, if the Bronx RHIO establishes a portal or other internet-based method that allows a patient, a patient's Personal Representative, or third party to Access Protected Health Information, the Bronx RHIO may not charge a fee for use of that system if no manual effort was required by the Bronx RHIO to fulfill the request.

D. Information about Minors. Access of patients, their Personal Representatives, their family members, their informal caregivers and their friends to Protected Health Information must be in accordance with laws granting minors the right to keep Minor Consent Information confidential from their parents or guardians. Notwithstanding Sections B and C, above, if the Bronx RHIO does not have a practical means of ensuring that Minor Consent Information can be segregated or otherwise filtered from other Protected Health Information about ~~minors~~ a minor who is age 10 or older and the Information Blocking Rule requirements at 45 C.F.R. § 171.204 are met, then the Bronx RHIO may deny Disclosure of all of such minor's Protected Health Information to such minor's Personal Representatives , family, informal caregivers, and friends ~~of minors between the ages of 10 and 17 with access to all of the minor's Protected Health Information~~.

E. In accordance with Section 1-3(III)(A)(5) of these Policies and Procedures, each Participant will provide patients with (i) notice – in a manner easily understood by patients – that their Protected Health Information is being uploaded to the RHIO System; (ii) a list of or reference to all Data Providers; (iii) information about how to contact said Data Providers; and (iv) a description of how patients may deny consent for all Participants to Access their Protected Health Information through the RHIO System.

F. The Bronx RHIO and its Participants shall participate in any applicable patient education programs developed by the Statewide Collaboration Process for the purpose of educating patients about the uploading of their Protected Health Information through the Bronx RHIO.

G. The Bronx RHIO will assure meaningful patient/consumer input and participation into its operations and decision-making.

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

I. The Bronx RHIO will require its Participants and Data Providers to notify the Bronx RHIO if, in response to a request by a patient, the Participant or Data Provider makes any corrections to the patient's erroneous information.

J. The Bronx RHIO will make reasonable efforts to provide its Participants with information indicating which other Participants have Accessed or received erroneous information that the Participant has corrected at the request of patients in accordance with Section I.

~~J.~~K. 5.6.4 If the Bronx RHIO determines that the error is due in part due to the Bronx RHIO's data aggregation and exchange activities (instead of solely due to an error in the underlying record maintained by the applicable Participant(s)), then the Bronx RHIO shall comply with Section III.L of Policy 1-7 (Audit Policy and Procedure).

Bronx RHIO, Inc.
Policy and Procedure
1-14
HIPAA Compliance

Adopted June 30, 2014
Amended and Restated as of February 28, 2017
Amended and Restated as of June 27, 2019
Amended and Restated as of April 29, 2021

I. Policy

While it is anticipated that most Participants will be Covered Entities and thus subject to the HIPAA Privacy Rule and HIPAA Security Rule, there may be some Participants that are not Covered Entities. The provisions of this section are designed to ensure that all entities that are not Covered Entities, other than a public health authority or a health oversight agency under HIPAA (45 CFR Sections 164.501 and 164.512(b) and (d)) Accessing Protected Health Information through the RHIO System abide by the same applicable HIPAA requirements as Covered Entities even if they are not otherwise legally obligated to do so.

II. Responsible Parties

The Executive Director will ensure the Bronx RHIO's compliance with this policy.

The Participants will have responsibility for complying with the applicable requirements of the HIPAA Privacy and Security Rules.

III. Procedure

A. Each Participant that is a Covered Entity shall comply with the HIPAA Privacy Rule and HIPAA Security Rule.

B. Each Participant that is not a Covered Entity, other than a public health authority or a health oversight agency under HIPAA (45 CFR Sections 164.501 and 164.512(b) and (d)), shall adopt/address all of the applicable administrative, physical and technical safeguards set forth in the HIPAA Security Rule as well as the restrictions on the use and Disclosure of Protected Health Information set forth in the HIPAA Privacy Rule.

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

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

2. The Bronx RHIO and its Participants may Transmit Protected Health Information to a Community-Based Organization that is not a Covered Entity only if the patient has executed an Affirmative Consent that permits Disclosure to such Community-Based Organization. The exceptions to the Affirmative Consent requirement set forth in Policy 1-3, including the exception for Patient Care Alerts, shall not apply to such a Community-Based Organization.

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

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

Bronx RHIO, Inc.
Policy and Procedure
1-15
Sanctions

Adopted June 30, 2014
Amended and Restated as of June 27, 2019

I. Policy

Sanctions are an important mechanism for ensuring that Participants and Authorized Users comply with these Policies & Procedures. The provisions in this Section are designed to provide guidelines for the imposition of sanctions by the Bronx RHIO and its Participants while leaving flexibility for the Bronx RHIO and its Participants to determine appropriate sanctions on a case by case basis.

II. Responsible Parties

The Patient Rights and Member Responsibilities Committee will ensure the Bronx RHIO's compliance with this policy.

The Participants will have responsibility for determining sanctions for individual Authorized Users in consultation with the Bronx RHIO as appropriate.

III. Procedure

A. Each Participant shall inform its Authorized Users about the Bronx RHIO's sanctions policies.

B. The Bronx RHIO Patient Rights and Member Responsibilities Committee will apply sanctions to Participants in the event of violation by a Participant of these Policies and Procedures, a Bronx RHIO Participation Agreement or of the QE Policies and Procedures. Sanctions may include suspending or terminating a Participant's participation in the RHIO and/or the assessment of fines or other monetary penalties. When determining the type of sanction to apply, the Patient Rights and Member Responsibilities Committee shall take into account the following factors: (i) whether the violation was a first time or repeat offense; (ii) the level of culpability of the Participant, e.g., whether the violation was made intentionally, recklessly or negligently; (iii) whether the violation

constitutes a crime under state or federal law; and (iv) whether the violation resulted in harm to a patient or other person.

C. Each Participant will apply sanctions to its Authorized Users in the event of violation of these Policies and Procedures, a Bronx RHIO Participation Agreement or of the QE Policies and Procedures. Sanctions may include (i) requiring an Authorized User to undergo additional training with respect to participation in the Bronx RHIO; (ii) temporarily restricting an Authorized User's Access to the RHIO System; or (iii) terminating the Access of an Authorized User to the RHIO System. When determining the type of sanction to apply, the Participant shall take into account the following factors: (i) whether the violation was a first time or repeat offense; (ii) the level of culpability of the Authorized User, e.g., whether the violation was made intentionally, recklessly or negligently; (iii) whether the violation constitutes a crime under state or federal law; and (iv) whether the violation resulted in harm to a patient or other person.

Bronx RHIO, Inc.
Policy and Procedure
1-16
Monitoring and Enforcement of SHIN-NY Compliance

Adopted June 30, 2014

I. Policy

The Bronx RHIO is required to comply with applicable federal and state law and with the Certification Requirements that Qualified Entities must satisfy to participate in the SHIN-NY (the "Certification Requirements"). The Bronx RHIO is also required to establish policies and procedures for receiving complaints from Participants and SHIN-NY stakeholders regarding possible non-compliance by the Bronx RHIO with applicable federal and state law and with the Certification Requirements; to investigate instances of non-compliance; and to make reports to the oversight agency responsible for overseeing compliance by Qualified Entities with federal and state laws and with the Certification Requirements (the "Oversight Entity"). This policy sets forth a process by which the Bronx RHIO will comply with these obligations.

II. Responsible Parties

The Executive Director will ensure the Bronx RHIO's compliance with this policy, including ensuring that Participants are notified of the existence of this Monitoring and Enforcement Policy.

The Bronx RHIO Executive Director will also notify the entity designated by the New York State Department of Health to oversee the certification process (the "Certification Body") of changes in this Policy in accordance with Section 7.11 of the Qualified Entity Organizational Characteristics Requirements.

The Participants will have responsibility for complying with this policy.

III. Procedure

A. Self-Audit

1. The Bronx RHIO will perform, or will cause a third-party to perform, an audit (a "Self- Audit") in order to verify its compliance

1776 Eastchester Rd., Suite 200, Bronx, NY 10461
Phone 718-708-6630 Fax 718-708-7272

with applicable federal and state law and with the Certification Requirements at least once per year, as required by the Oversight Entity and as stated in the Privacy & Security Policies and Procedures Section 6.2.4 and in Article 1-7 of these Policies and Procedures.

2. The scope of the Self-Audit will include a review of the Bronx RHIO's compliance with applicable federal and state laws and with the Certification Requirements and a review of Participants' compliance with applicable SHIN-NY Policy Guidance.

B. **Process for Accepting Complaints**

1. The Bronx RHIO will receive, investigate and respond to complaints from SHIN-NY stakeholders, including Participants.

2. Any SHIN-NY stakeholders, including any Participant, may file with the Bronx RHIO a complaint of any suspected non-compliance with applicable federal or state laws or with the Certification Requirements. The complaint (the "Non-Compliance Complaint") must be in writing and must include the following information if known:

   a. the suspected non-compliance;

   b. the acts or omissions believed to constitute non-compliance;

   c. the name of the QE involved;

   d. the name of the Participant involved, if any;

   e. all dates related to the suspected non-compliance; and

   f. all locations related to the suspected non-compliance, if any.

3. A Non-Compliance Complaint related to the Bronx RHIO or a Participant must be filed within 180 days from the date the complainant knew or should have known that non-compliance occurred for the Non-Compliance Complaint to be subject to investigation under this Policy.

4. If a Non-Compliance Complaint related to the Bronx RHIO or a Participant is filed with the Bronx RHIO, the RHIO will conduct an Internal Investigation in accordance with Section C below.

5. If a complaint is not a non-compliance issue, it will be addressed in a manner deemed appropriate by the Bronx RHIO's Executive Director.

C. **Internal Investigation Process**

1. If the Bronx RHIO becomes aware of potential non-compliance or receives notice of a Non-Compliance Complaint, the Bronx RHIO will conduct an internal investigation (an "Internal Investigation") of such complaint to determine whether non-compliance has occurred.

2. The Bronx RHIO will begin the Internal Investigation within 30 days after becoming aware of potential non-compliance or receiving notice of a Non-Compliance Complaint.

3. The Bronx RHIO will complete the Internal Investigation as soon as reasonably practicable but in any event no later than 60 days after becoming aware of potential non-compliance or receiving notice of a Non-Compliance Complaint.

D. **Reporting to Oversight Entity**

1. Following an Internal Investigation conducted pursuant to Section C above, the Bronx RHIO will report to the Oversight Entity in writing the existence of any non-compliance immediately after the Bronx RHIO determines that non-compliance has occurred. The report (the "Non-Compliance Report") will describe the non-compliance and any harmful effects known to the Bronx RHIO (including a list of Participants harmed, if any) resulting from non-compliance.

2. If instructed by the Oversight Entity to perform an Internal Investigation (rather than if the Bronx RHIO chose to undertake the investigation voluntarily under Section C above), the Bronx RHIO will report the results of such investigation to the Oversight Entity. If the Bronx RHIO did not detect non-compliance as a result of such Internal Investigation, the Bronx RHIO will provide to the Oversight Entity a statement that no non-compliance was detected and a summary of the Internal Investigation conducted outlining the investigation findings.