Santa Cruz Health Information Organization (SCHIO)

Policies and Procedures

June 2015

Revised April 1, 2017

Table of Contents

1 INTRODUCTION AND OVERVIEW OF POLICIES AND PROCEDURES

1.1 Introduction

1.1.1 Description of Health Information Exchange Organization ("SCHIO")

SCHIO is Santa Cruz Health Information Exchange, LLC a California Corporation, organized by Health Care Stakeholders in Santa Cruz County each of whom have executed a participation agreement with the SCHIO, and all of which agreements contain substantially similar terms and conditions (by July 2016) to facilitate health information sharing and aggregation of patient health information for treatment, payment, operations, public health and other lawful purposes in a manner that complies with all applicable laws and regulations, including without limitation those protecting the privacy and security of health information and which participation agreement is further defined in Section 1.2 below (the "Participation Agreement"). The obligations of a party under these Policies and Procedures are in addition to a party's obligations under its Participation Agreement.

1.1.2 Development of Policies and Procedures

SCHIO is solely responsible for the development of the Policies and Procedures and may implement any new SCHIO Policies and Procedures, or amend, or repeal and replace any existing SCHIO Policies and Procedures, in whole or in part as provided in the Participation Agreement.

SCHIO shall provide Participant notice of changes to the Policies and Procedures by electronic mail, but it is each Participants' responsibility to keep informed of and compliant with the newest versions of the SCHIO Policies as posted on the SCHIO website.

1.2 Definitions

For the purposes of these Policies and Procedures, the Capitalized terms shall have the meaning given in the Participation Agreement or the Business Associate Agreement, as applicable unless otherwise defined herein. following terms shall have the meanings set forth below:

1.2.1. "Additional Services" means products and/or services not expressly described in the Participation Agreement that the SCHIO offers to certain Participants from time to time, and described in these Policies and Procedures and/or the applicable Participation Agreement.

1.2.2. "Authorized Users" shall mean those persons who have been authorized to access Patient Data through the System. "Authorized Users" may include, but are not limited to, health care providers and employees, staff, contractors, or agents of a Participant.

1.2.3. "CMIA" means the California Confidentiality of Medical Information Act, California Civil Code Section *56 et. seq.*

1.2.4. Data Provider" means a Participant that is registered to provide data to the SCHIO for use through the Services.

1.2.5. "Data Recipient" means a Participant that uses the Services to obtain or access health information.

1.2.6. "Participant" means a party that entered into a Participation Agreement with the SCHIO to act as a Data Provider and/or as a Data Recipient.

1.2.7. "Participant Type" means the category(ies) of Participant to which a particular Participant is assigned by SCHIO based upon that Participant's role in the health care system.

1.2.8. "Participation Agreement" means a legally binding agreement between SCHIO and a party pursuant to which the party acts as a Participant in accordance with, and agrees to comply with, the Participation Agreement and these Policies and Procedures.

1.2.9. "Patient Data" means information provided, or made available for exchange by a Data Provider through HIO's System and Services.

1.2.10. "Permitted Purposes" means a Data Recipient.

1.2.11. "Policies and Procedures" means, collectively, the policies and procedures adopted by SCHIO for the operation and use of the System and Services, including without limitation any operations manual, privacy and /or security policies, and technical specifications for the System and/or the Services all of which shall be in accordance with the Participation Agreement.

1.2.12. "Services" means the health information exchange and related services.

1.2.13. "System" means the technology, including but not limited to platforms and interfaces, provided or made available by the SCHIO.

2 SYSTEM AND SERVICES

2.1 Downtime.

SCHIO contracts for hosted services that guarantee at least 99.9% uptime per calendar month, not including scheduled downtime. For each calendar year, scheduled hardware, software, and communications maintenance SCHIO will use commercially reasonable efforts to limit unscheduled downtime to an average of [eight (8) hours] in total per calendar month or less. All scheduled maintenance will be carried out on dates and at times published by SCHIO with at least five (5) business days' advance notice to all Participants via e-mail or other electronic method, or published on its website at: www.santacruzhie.org.

2.2 Permitted Purposes for Use of System and Services

Participants and Authorized Users may access and use data through SCHIO only for permitted purpose(s), as defined in the Participation Agreement. In general, requests for access to and the use of patient health information from the SCHIO will be permitted for a Permitted Purpose, such as for treatment, payment, health care operations, public health and the determination of eligibility for government benefits.

2.3 Minimum Necessary Access to Patient Data

An Authorized User shall use the System and the Services to request or seek access to only that amount of Patient Data that the Authorized User is permitted to request pursuant to Applicable Laws.

a. Authorized Users shall provide or request health information through the SCHIO only to the extent necessary and only for those purposes that are permitted by applicable federal, state and local laws and regulations;

   Under no circumstances may information be requested for a discriminatory purpose.

b. No services to Third Party: Recipient shall use the System or the Services pursuant to its Participation Agreement and only for the Authorized User's own account, and shall not use any part of the System or the Services to provide separate services or sublicenses to any entity that will be deemed a third party under its Participation Agreement, including without limitation providing any service bureau services or equivalent services to a third party.

c. No Services Prohibited by Law: The Authorized User shall not use the System or the Services for which the Participant has registered for any purpose or in any manner that is prohibited by federal law or by the laws of the State of California.

d. No Use for Comparative Studies: An Authorized User shall not use the System or the Services to aggregate data to compare the performance of Participants and/or Authorized Users, without the express written consent of SCHIO and each of the Participants and Authorized Users being compared.

3 PARTICIPANTS DUTY TO MONITOR ACCESS TO THE SYSTEM

3.1 Participant Audits and Monitoring

Each Participant shall monitor and audit access to and use of their information technology systems that connect with the SCHIO to ensure access to the System and use of Patient Data complies with the Participation Agreement and Applicable Law. Participant will provide SCHIO with monitoring and access records as reasonably requested by SCHIO for auditing purposes.

3.2 Audit Logs

SCHIO will make available audit logs to each Participant with respect to its Authorized Users pertaining to access to or use of Patient Data or permit Participants to query for the equivalent information.

4 AUTHORIZED USERS AND AUTHENTICATION

4.1 Required Information for Authorized Users

Authorization is the process of determining whether a particular Authorized User within a Participant has the right to access Protected Health Information via the System. Authorization is based on role-based access standards that take into account an individual's job function and the information needed to successfully carry out a role within the Participant. This Section sets forth minimum requirements that Participants shall follow when establishing role-based access standards and authorizing individuals to access information to the minimum necessary for accomplishing the intended purpose of the exchange, thereby allowing patients to have confidence in the privacy of their health information as it moves between Participating Entities.

4.2 General

The purpose for which an Authorized User may access information via the System and the types of information an Authorized User may access shall be based, at a minimum, on the Authorized user's job function and relationship to the patient.

4.3 Role-Based Access Standard

Participants shall establish and implement policies and procedures that:

a. Establish categories of Authorized Users;

b. Define the purposes for which Authorized Users in those categories may access Patient Data via the System, consistent with the limitation set forth in the Participation Agreement; and

c. Define the types of Patient Data that Authorized Users within such categories may access (e.g., demographic data).

4.4 Training

The Participant shall provide appropriate and adequate training to all of the Participant's personnel, including without limitation Authorized Users, in the requirements of Applicable Laws..

4.4.1 Training Materials

SCHIO will provide training materials for Participants use in training Authorized Users in the technical aspects of use of the System. SCHIO will make virtual training available through its website, in addition to other training materials as deemed appropriate.

4.4.2 SCHIO Training Responsibility

Participants shall provide on-site training, web-based training, or comparable training tools to ensure that Authorized Users are familiar with these SCHIO Policies and Procedures governing access to information via the System. This training may be provided in conjunction with the Participant's regular HIPAA training activities.

4.4.3 Participants Training Responsibility

Participants shall ensure that each Authorized User undergoes the training specified in section [Training].

4.4.4 Training Documentation Retention

Participants shall ensure that each Authorized User has received training and will comply with these Policies and Procedures, Participation Agreement, and Participant's own privacy and security policies and procedures. Documentation shall be retained by Participants for at least [six (6) years] and made available to SCHIO within thirty (30) days of written request.

4.5 Support

Telephone and/or E-Mail Support. SCHIO shall provide, by telephone and/or e-mail, during normal business hours, support and assistance in resolving difficulties in accessing and using the System and the Services.

5 SECURITY OF PATIENT DATA

5.1 Standards

SCHIO and each Participant shall comply with the standards for the privacy and security of patient health information, including without limitation protected health information described in HIPAA and medical information described in the CMIA.

5.2 SCHIO shall store Patient Data on secure computers located in a physically secure data center.

5.3 Data in Transit

The Participant agrees to ensure that all data in transit shall be encrypted at least at a minimum to meet HIPAA requirements.

5.4 Best Practices

The Participant shall review and require each of its Authorized Users to review, the SCHIO Security Best Practices document available at www.santacruzhie.org.

5.5 Reporting of Breaches and Security Incidents

SCHIO and Participant shall notify the other regarding any misuse or inappropriate disclosure of Patient Data of which SCHIO or Participant becomes aware, any security incident (other than an Unsuccessful Security Incident) concerning electronic Patient Data

and any Breach of Privacy or Security. This notification shall be made promptly without unreasonable delay and in no case no later than 24 hours after the notifying party becomes aware of the incident.

5.5.1 Reporting Unsuccessful Security Incidents

The Participant shall provide a report annually to the SCHIO, describing in summary form, the nature and extent of Unsuccessful Security Incidents directly related to the SCHIO that were experienced by the Participant during the period covered by that report.

5.5.2 Reports to Participants

SCHIO shall on a monthly basis provide a report to all Participants describing all Serious Breaches of Privacy or Security discovered by the SCHIO or reported by Participants to SCHIO during the prior month. SCHIO shall on an annual basis provide a report to all Participants describing in summary form Unsuccessful Security Incidents reported by Participants to SCHIO.

6 PRIVACY OF PATIENT DATA

6.1 Consent and/or Authorization Requirements

Each patient in the system has an attribute for elective choice or Consent and/or specific Authorization Requirements. For each patient maintained on the System the privacy and consent profile function provides a mechanism to record the patient privacy consent choice and a method to enforce the privacy consent appropriate to the use.

6.1.1 Obtaining Patient Consent

The default consent status for Patients in the System is to share patient health information with other SCHIO Participants.

6.1.2 Steps to obtain Patient consent

Once a Patient has been identified by a Participant's registration staff, the Participant offers the Patient a Patient Consent form. The SCHIO can accommodate two consent statuses: Opt-In which means share all PHI, opt-out of sharing all PHI except for the purposes of emergency medical services and for purposes of reporting required by law.

a. Once the patient or the patient's guardian signs the opt-out form, an Authorized User updates the patient's record in their EHR.

b. The Participant shall store a copy of the consent form to be retrieved in case of an audit.

c. A Patient may change their SCHIO consent status at any time by completing a new consent or opt-out form with a more recent date than the previous consent or opt-out form.

6.2 Permitted Uses of Patient Data

Participants shall advise Authorized Users to access the System and the Services only to locate and retrieve Patient Data only for the purpose(s) specified in the Participant Agreement and in no event in any manner that is prohibited by applicable laws.

6.2.1 Access

Access controls govern when and how the system and Patient information may be accessed by Authorized Users. This section sets forth minimum controls Participants shall implement to ensure that: (1) only Authorized Users access information via the System; and (2) they do so only in accordance with the requirements specified herein that limit their access to specified information. These access controls are designed to minimize unauthorized access and ensure that Patient Data is used for authorized purposes.

6.2.2 Authorized Users

Participant shall be responsible for communicating to SCHIO in writing all users that are authorized to access the System and Services.

Participant will identify an authorized delegate within its organization authorized to request user access to the System. Authorized delegates are responsible for communicating to SCHIO any changes that would affect an authorized users right to access Patient Data, including but not limited to role changes, access privileges and termination of employment of Authorized Users.

6.2.3 Access Specifications

SCHIO shall provide each Authorized User with a unique System user name and the ability to select a unique password to access Patient Data via the System.

Authorized Users shall be authenticated in accordance with the provisions of Section [Authentication].

6.2.4 Group or temporary user names shall be prohibited

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

6.2.5 Access Limited to Minimum Necessary Information.

Participants shall ensure that reasonable efforts are made to limit the information accessed via the System to the minimum amount necessary to accomplish the intended purpose for which the information is accessed.

6.2.6 Termination of Access and Other Sanctions

Participants shall develop policies and procedures to terminate the access of Authorized Users and/or to impose sanctions as necessary.

Participants shall ensure that an Authorized Users' access to the System is terminated in the following situations and in accordance with the processes described:

a. Immediately or as promptly as reasonably practicable but in any event within one business day of termination of a Participant's Organizational Participation Agreement with the SCHIO;

b. Immediately following an Authorized User's breach of the Authorized User Agreement and/or;

c. Immediately or as promptly as reasonably practicable but in any event within one business day of notification of termination of an Authorized User's employment or affiliation with the Participant.

Participants shall notify SCHIO immediately via email upon termination of an Authorized User's access to the System.

6.3 Permitted [and Prohibited] Uses and Disclosures of Patient Data.

An Authorized User may use and disclose Patient Data acquired through the use of the System and the Services as and to the extent permitted by Applicable Law.

6.4 Limitations on Disclosure of Patient Data

Certain sensitive health information may be restricted from disclosure by state and federal law. Participants are responsible for complying with applicable laws and for filtering any information that should not be disclosed to other Participants through the SCHIO without a Patient's written authorization.

7 EXCHANGE OF PATIENT DATA

7.1 Measures to Assure Accuracy of Data

Each Data provider shall use reasonable and appropriate efforts to ensure the accuracy and completeness of the Patient Data it provides through the System.

7.2 Query/Retrieve Mode of Exchange.

SCHIO operates a Query/Retrieve mode of exchange which can solicit data from other HIOs. This means that an Authorized User may query another HIE/HIO for Patient Data in which there is a treatment relationship.

8 TECHNOLOGY

8.1 Associated Technology

Each Participant shall be responsible for procuring all hardware and software necessary for it to access the System.

Participant shall be responsible for ensuring that all computers used to access the System and Services are appropriately configured, including but not limited to:

- relevant operating system;
- supported web browser versions;
- appropriate security measures, including but not limited to, up-to-date anti-virus and firewall software.

Participant shall provide notice and complete details on any changes to an interface between the System and Participants' system. Notice shall be provided to SCHIO, in writing, prior to the intended change.

9 SCHIO OPERATIONS

9.1 SCHIO's Privacy and Security Standards

9.1.1 Policies and Procedures

SCHIO requires that each Participant enter into a Participation Agreement prior to being granted access to or use of the System.

9.1.2 Technical, Administrative and Physical Safeguards

a. Master Patient Index

The System's Master Patient Index ("MPI") is the directory of all patients. Each MPI record contains the patient's demographic data and can be used to identify matching clinical information for that patient from each Participant.

b. Adding a New Patient Record

To add a patient to the MPI, a Participant data feed must include patient's first and last name, the Patient's date of birth, Participant's medical record number, street address, and the Patient's gender. Some interfaces between Participant's system and the System will automatically add Patients to the MPI.

c. Patient Matching

The System uses rules to compare incoming patient data to existing patient that already exist in the System. If a match can be established with sufficient confidence, the System creates an association and links the incoming record to the existing patient. If the System cannot establish with sufficient confidence that the incoming patient data matches an existing patient, a new patient record is created and the record is linked to the new record.

d. Duplicate Records

Records of the same Patient available through the System may be merged:

i. Automatically by the System

ii. Upon an Authorized User's request

iii. Manually by the HIO technical team

9.2 Audits and Reports

SCHIO shall perform audits and provide reports to each Participant according to the applicable Participation Agreement and these Policies and Procedures.

Audits are useful oversight tools for recording and examining access to information through the System (e.g., who accessed what data and when) and are necessary for verifying compliance with access controls, like those specified in Section [Access], developed to prevent/limit inappropriate access to information. This section sets forth a minimum requirement that Participants shall follow for audits regarding access to health information via the System.

9.2.1 SCHIO Audits

SCHIO or a third party engaged by SCHIO may audit a Participant on a periodic basis. The purpose of these audits will be to confirm compliance with and proper use of the System in accordance with the Participation Agreement and these SCHIO Policies and Procedures.

SCHIO audits and provides reports on the following:

a. Participants. List of current Participants are available on the SCHIO website.

b. Usage Reports. Statistical reports regarding the Participant's usage of the Services.

c. Reports to Public Agencies. Reports that certain Participants may be required to make to public health agencies.

d. Audit Trail Reports. Reports that pertain to audit trail tracking.

9.2.2 Conduct of Audits

Audits will take place during normal business hours and at mutually agreeable times and shall be limited to such records, personnel and other resources of Participant as are necessary to determine proper use of the System, compliance with Participant's Participation Agreement, or these SCHIO Policies and

Procedures, or to comply with applicable state or federal requirements. Such audits will be performed in a manner designed to reasonably minimize interference with Participant's day-to-day operations.

9.3 Digital Certificates

SCHIO's network administrator manages digital certificates and the renewal or replacement of those certificates.

9.4 Endpoint Changes

SCHIO's network administrator shall coordinate any changes to service endpoint information to the Services Registry Manager twenty-four (24) hours prior to making any change.

9.5 Services Registry Information Caching and Sharing

SCHIO will cache Services Registry information, but shall not provide cached information to others. The cache shall be refreshed at least every twenty-four (24) hours.