SCHIEx POLICIES AND PROCEDURES

Revised January 16, 2020

Participants who have executed a SCHIEx Participation Agreement and Business Associate Agreement and have agreed to the terms and conditions stated therein must comply with the following SCHIEx Policies and Procedures.

A Participant's failure to comply with the SCHIEx Policies and Procedures stated below constitutes a breach of the SCHIEx Participation Agreement and may result in termination of the Agreement, denial of access to the SCHIEx network, or financial penalties as discussed in the SCHIEx Participation Agreement and herein.

These SCHIEx Policies and Procedures may be revised and updated periodically in accordance with the Participation Agreement and the SCHIEx Policy Manual (as defined below) in response to changes in applicable laws and regulations, changes in technology and standards, or other factors affecting the governance and operation of SCHIEx. Notice will be given to all Participants electronically by means of an electronic mail message sent to the electronic mail address submitted by the Participant and by notice posted on the SCHIEx website. The current version of the SCHIEx Policies and Procedures will be available on the SCHIEx website. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Policies and Procedures.

As discussed in more detail below, compliance with and adherence to these Policies and Procedures will be Monitored and enforced by South Carolina Health Information Partners, Inc. ("SCHIP" or "Governing Authority"). Any suggested additions or changes to these Policies and Procedures should be submitted to the Governing Authority for consideration.

THESE POLICIES AND PROCEDURES ARE REQUIRED FOR PARTICIPATION IN SCHIEX. THESE POLICIES AND PROCEDURES DO NOT SUPPLANT OR PREEMPT ANY FEDERAL AND STATE LAWS APPLICABLE TO HEALTH CARE PROVIDERS OR OTHER ENTITIES. FOLLOWING THESE POLICIES AND PROCEDURES DOES NOT PROTECT A PARTICIPANT OR ANOTHER ENTITY FROM LIABILITY UNDER APPLICABLE LAW.

SCHIEX IS INTENDED TO BE USED AS AN INFORMATION GATHERING TOOL TO AID HEALTH CARE PROVIDERS AND OTHER PARTICIPANTS. THE USE OF SCHIEX DOES NOT ELIMINATE A PROVIDER'S NEED TO EXERCISE PROFESSIONAL JUDGMENT IN CLINICAL DECISION MAKING. SCHIEX DOES NOT WARRANT OR GUARANTEE THE ACCURACY OR COMPLETENESS OF THE INFORMATION MADE AVAILABLE FROM PARTICIPANTS THROUGH SCHIEX.

1. Definitions.

Terms used in this Agreement that are specifically defined in the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), or the Health Information Technology for Economic and Clinical Health Act ("HITECH") enacted as part of the American Recovery and Reinvestment Act of 2009, and their attendant regulations and guidance, shall have the same meaning as set forth in HIPAA, unless expressly stated otherwise herein. A change to HIPAA which modifies any defined HIPAA term, or which alters the regulatory citation for the definition, shall be deemed incorporated into this Agreement.

a. **Adapter** means the "system" that holds a data provider's patient demographic and clinical data, identifies that data to a statewide Record Locator Service (Enterprise Master Patient Index) and allows for a "real time" sharing of clinical information (based on role-based access controls) from disparate electronic data contained on other linked Adapters.

b. **Adverse Security Event** means the the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content while Transacting such Message Content in a manner permitted by this Agreement. The term ''Breach'' includes access anyone who is not a Participant or Participant User or by a Participant or Participant User in any manner that is not a Permitted Purpose under this Agreement. For the avoidance of doubt, an "Adverse Security Event" under this Agreement does not include the following:

(1) any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Participant or Participant User if—

(I) such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and

(II) such unencrypted Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or

(2) any acquisition, access, disclosure or use of information contained in or available through the Participant's System where such acquisition, access, disclosure or use was not directly related to Transacting Message Content.

c. **Applicable Law** means (i) for the Participants that are not Federal Participants, all applicable statutes and regulations of the State(s) or jurisdiction(s) in which the Participant operates, as well as all applicable Federal statutes, regulations,

standards and policy requirements; (ii) for the Federal Participants, all applicable Federal statutes, regulations, standards and policy requirements.

d. **Audit** shall mean a review and examination of records (including logs), and/or activities to ensure compliance with the Participation Agreement and the SCHIEx Policy Manual and to ensure accuracy of the data transmission and conversion of data by the Adapter. This review can be manual, automated or a combination of both.

e. **Authorization** has the meaning and includes the requirements and have the meaning set forth at 45 CFR § 164.508(b) of the HIPAA Regulations and includes any similar but additional requirements under Applicable Law.

f. **Authorized User** means any person who has been authorized to Transact Message Content through a respective Participant's System in a manner defined by the respective Participant. Authorized Users may include, but are not limited to, Health Care Providers; Health Plans; individuals whose health information is contained within, or available through, a Participant's System; and employees, contractors, or agents of a Participant. A Participant User may act as either a Submitter, Recipient or both when Transacting Message Content. Authorized Users receive their rights to use SCHIEx services either by registering as Participants themselves or by executing a Participant User Agreement with an organization that registers as a Participant and designates individuals who will be authorized to use the SCHIEx services on the Participant's behalf. For example, an Authorized User may be an individual physician who registers as a Participant. In addition, an Authorized User may be a member of that physician's office staff designated by the physician, or any one of a number of a hospital's employees and/or medical staff members authorized by the hospital to act as Authorized Users under the hospital's registration as a Participant.

g. **Clinical Viewer** means the web-based interactive data organization and visualization dashboard application, which may be used by Participants in connection with data exchanged or obtained via SCHIEx.

h. **Confidential Participant Information,** for the purposes of this Agreement, means proprietary or confidential materials or information of a Discloser in any medium or format that a Discloser labels as such upon disclosure. Confidential Participant Information includes, but is not limited to: (i) the Discloser's designs, drawings, procedures, trade secrets, processes, specifications, source code, System architecture, security measures, research and development, including, but not limited to, research protocols and findings, passwords and identifiers, new products, and marketing plans; (ii) proprietary financial and business information of a Discloser; and (iii) information or reports provided by a Discloser to a Receiving Party pursuant to this Agreement. Notwithstanding any label to the contrary, Confidential Participant Information does not include Message Content; any information which is or becomes known publicly through no fault of a Receiving Party; is learned of by a Receiving Party from a third party entitled to disclose it; is already known to a Receiving Party before receipt from a Discloser as documented by Receiving Party's written records; or, is independently developed by Receiving Party without reference to, reliance on, or use of,

Discloser's Confidential Participant Information. Message Content is excluded from the definition of Confidential Participant Information because other provisions of the DURSA address the appropriate protections for Message Content.

i. **Data** shall mean that information which is requested or sent by a Participant to another Participant through SCHIEx. This includes, but is not limited to, PHI, de-identified data, pseudonymized data and metadata.

j. **DURSA** means the Third Restatement of the Data Use and Reciprocal Support Agreement. The DURSA is a comprehensive, multi-party trust agreement that will be signed by entities wishing to participate in the eHealth Exchange. The DURSA provides the legal framework governing participation in the eHealth Exchange by requiring the signatories to abide by a common set of terms and conditions. These common terms and conditions support the secure, interoperable exchange of health data between and among eHealth Exchange participants across the country.

k. **eHealth Exchange** (formerly known as the Nationwide Health Information Network or NwHIN) means the data sharing network which was developed under the auspices of the Office of the National Coordinator for Health Information Technology and consists of governmental and non-governmental exchange partners who share information under a multi-purpose set of standards and services which are designed to support a broad range of information exchange activities using various technical platforms and solutions

l. **Electronic Protected Health Information** or **(EPHI)** has the same meaning as the term "electronic protected health information" in 45 CFR §160.103, and shall include, without limitation, any EPHI provided by a Covered Entity or created or received by a Business Associate on behalf of a Covered Entity.

m. **Executive Director** means the Executive Director of SCHIP.

n. **Federal Participants** means those Participants that are federal agencies.

o. **Governing Authority** means South Carolina Health Information Partners, Inc., a South Carolina nonprofit corporation, which is responsible for administering SCHIEx and fulfilling the roles and responsibilities described herein.

p. **Health Care Operations** has the meaning set forth in 45 C.F.R. § 164.501 of the HIPAA Regulations.

q. **Health Information Organization (HIO)** means an organization that oversees and governs the exchange of health-related information among Health Care Organizations according to nationally recognized standards.

r. **Health Care Provider** has the meaning set forth in 45 C.F.R. § 160.103 of the HIPAA Regulations.

s. **Health Plan** has the meaning set forth in 45 C.F.R. § 160.103 of the HIPAA Regulations

t. **Health Information Exchange (HIE)** means the electronic movement of health-related information according to nationally recognized standards

u. **HIPAA** means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, as amended, and related HIPAA regulations (45 CFR. Parts 160-164).

v. **HIPAA Regulations** means the Standards for Privacy of Individually Identifiable Health Information and, the Security Standards for the Protection of Electronic Protected Health Information and the Breach Notification Rule (45 C.F.R. Parts 160 and 164) promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as in effect on the Effective Date of this Agreement and as may be amended, modified, or renumbered.

w. **HITECH** means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII and Title IV of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, as amended, and related regulations.

x. **Individual** means the person who is the subject of PHI, usually a patient, and whose PHI is transmitted by Participants via SCHIEx, or that person's legal guardian or other legal representative.

y. **Individually Identifiable Health Information** means information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer or health care clearinghouse and relates to the past, present 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 that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Individually Identifiable Health Information shall have the same meaning as the term is defined in 45 C.F.R. § 160.103.

z. **Message** means a mechanism for exchanging Message Content between Participants via SCHIEx's Record Locator Service, which complies with the SCHIEx Performance and Service Specifications. Messages are intended to include all types of electronic transactions in the exchange including but not limited to requests, assertions, responses, and notifications, as well as the data or records transmitted with those transactions.

aa. **Message Content** means that information contained within a Message or accompanying a Message using the Specifications. This information includes, but is not limited to, Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonymized data, metadata, Digital Credentials, and schema.

bb. **Monitor** shall mean a review and examination of records (including logs), and/or activities to evaluate the utilization levels, efficiency and technical capabilities of SCHIEx. This review can be manual, automated or a combination of both.

cc. **Notice** and **Notify** means a notice in writing sent to the appropriate Participant's representative at the address listed in the Participation Agreement, to the Governing Authority, or to an Individual, as applicable.

dd. **Optional Services** are services that SCHIEx may provide Participants who choose to contract and pay for such services in addition to the core services provided in SCHIEx EXCHANGE and SCHIEx DIRECT and covered under the terms of the Participation Agreement. Optional Services will be approved by the Governing Authority and posted on the SCHIEx website.

ee. **Participant** means (i) an organization that oversees and conducts, on its own behalf and/or on behalf of its Participant Users, electronic transactions or exchanges of health information among groups of persons or organizations, including but not limited to, HIOs; (ii) a federal, state, tribal or local government, agency or instrumentality that needs to exchange health information with others as part of their official function; (iii) an organization that supports program activities or initiatives that are involved in healthcare in any capacity and has the technical ability to meet the applicable Performance and Service Specifications to electronically transact health information on its own behalf or on behalf of its Participant Users and has the organizational infrastructure and legal authority to comply with the obligations in this Agreement and to require its Participant Users to comply with applicable requirements in this Agreement. All Participants must enter into a Participation Agreement with SCHIEx or Restatement III of the Data Use and Reciprocal Support Agreement with the eHealth Exchange and abide the terms and conditions contained therein.

ff. **Participant Member** means a member of an HIO that is a Participant of SCHIEx. A Participant Member must execute a Participation Agreement and pay the requisit Participation Fee as set forth on the Fee Schedule, but the HIO may pay the fee on behalf of its Participant Members. A Participant Member must adhere to all requirements for Participants stated in these SCHIEx Policies and Procedures.

gg. **Participation Agreement** shall mean the underlying SCHIEx Participation Agreement entered into between each Participant and SCHIEX, which outlines the terms of the SCHIEx services and describes the duties and responsibilities of each Participant and SCHIEx.

hh. **Payment** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

ii. **Permitted Purpose** shall mean one of the following reasons for which Participants, Participant Members, and Authorized Users may legitimately exchange Data through SCHIEx. Permitted Purposes for SCHIEx DIRECT include any exchange of Data related to the provision of health care to the extent permissible under all

applicable law, including but not limited to Treatment, Payment, operations, public health reporting, and quality reporting. Permitted Purposes for SCHIEx EXCHANGE are limited to the following:

(a) Treatment, Payment, and Health Care Operations as defined by HIPAA

(b) Any disclosure based on an Authorization by the individual whose PHI is included in the Transaction of Message Content;

(c) Transaction of Message Content related to value based payment models, alternative payment arrangements or financial risk sharing models of any nature whether for Medicare, Medicaid, other federal programs, commercial payers or employer self-insured arrangements. This could include, but is not limited to, participation in Medicare bundled payments, the Medicare Shared Savings Program, other Medicare Alternate Payment programs, Medicaid Managed Care programs or commercial value-based payment programs;

(d) Transaction of Message Content for certain specialized government functions which are necessary to fulfill an agency's statutory obligations for programs the agency administers including, but not limited to: (i) activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission; (ii) for the purpose of the Department of Veterans Affairs determining the individual's eligibility or entitlement to benefits under the VA upon separation or discharge of the individual from military service; (iii) to determine eligibility for or entitlement to or provision of other government benefits; (iv) for activities related to eligibility for or enrollment in a health plan that is a government program; (v) for administering a government program providing public benefits, to coordinate covered functions; or, (vi) to improve administration and management relating to the covered functions of such government programs;

(e) Public health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e) , including but not limited to submission of immunization, communicable disease, and cancer reporting to federal and state agencies;

(f) Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content under this Agreement, provided that the purpose is not otherwise described in subsections 1-46 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA Regulations. "Meaningful use of certified electronic health record technology" shall have the meaning assigned to it in the regulations promulgated by the

Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102; and Transaction of Message Content in support of an individual's: (i) right to access their health information or (ii) right to direct with whom their information can be shared or where their information should be sent. For the avoidance of doubt, a Participant may be prevented from disclosing information due to Applicable Law even though the individual asserts this Permitted Purpose;

jj. **Privacy Rule** shall mean the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information, which are codified at 45 C.F.R. Parts 160 and 164, Subparts A, C, and E, and any other applicable provision of HIPAA, and any amendments thereto, including HITECH.

kk. **Protected Health Information** (**PHI)** has the meaning given to the term under the Privacy Rule, including but not limited to, 45 C.F.R. § 160.103, and shall include, without limitation, any PHI provided by or received by a Authorized User. Unless otherwise stated in the Participation Agreement, any provision, restriction, or obligation in the Participation Agreement related to the use of PHI shall apply equally to EPHI.

ll. **Recipient** means the Participant(s), Participant Member(s) or Authorized User(s) who receives Message Content through a Message to a Recipeint for a Permitted Purpose.

mm. **Record Locator Service** (RLS) means the system that identifies and links patients with their data across the linked continuum of care.

nn. **Required By Law** shall have the meaning given to the term under the Privacy Rule including, but not limited to, 45 C.F.R. § 164.103, and any additional requirements created under HITECH.

oo. **SCHIEx** means the South Carolina Health Information Exchange.

pp. **SCHIEx EXCHANGE** means the secure, standards-compliant technology and policy framework that enables the electronic discovery, query, and retrieval of key clinical Data at the point of care. SCHIEx EXCHANGE functions such that Participants query and retrieve clinical Data directly from other Participants involved in a patient's care using standards-compliant electronic health record systems and SCHIEx technology services. Services associated with SCHIEx EXCHANGE include a statewide Master Patient Index, Record Locator Service, terminology standards and services, trusted uniform transport, Public Key Infrastructure certificate-based encryption and authentication, Audit/log of document transport between Participants, bi-directional exchange with the South Carolina Department of Health and Environmental Control Immunization Registry, RX (prescription) hub, access to the SCHIEx Nationwide Health Information Network Gateway, and other services approved by the Governing Authority and posted on the SCHIEx website from time to time.

qq. **SCHIEx DIRECT** means the secure, standards-compliant technology and policy framework that enables point-to-point transport of health Data via a directed Message sent from one Participant to an identified recipient. SCHIEx DIRECT functions such that Participants directly send or "push" a user-defined Message to a known and trusted receiver using an e-mail client or web portal and SCHIEx technology services. Services associated with SCHIEx DIRECT include SCHIEx DIRECT addresses, security and trust services, certificate-based encryption and authentication, Message transport and delivery, and other services approved by the Governing Authority and posted on the SCHIEx website from time to time.

rr. **SCHIEx Performance and Service Specifications** shall refer to the SCHIEx test approach and the SCHIEx interface specifications contained in the SCHIEx Policy Manual and as amended from time to time.

ss. **SCHIEx Policy Manual** means the documents approved by the Governing Authority containing these SCHIEx Policies and Procedures, the SCHIEx Performance and Service Specifications, the Participation Agreement, the Business Associate Agreement, and any other documents included by the Governing Authority. Each Participant is contractually bound to the contents of the SCHIEx Policy Manual, as it may be amended. The Governing Authority shall review and may amend the SCHIEx Policy Manual from time to time as provided in the Participation Agreement.

tt. **SCHIEx Policies and Procedures** shall mean the policies and procedures adopted by the Governing Authority that describe the management and operation of, and the terms for participation in, SCHIEx, contained herein and incorporated into the SCHIEx Policy Manual, as they may be amended from time to time.

uu. **Secretary** shall mean the Secretary of the United States Department of Health and Human Services or his designee.

vv. **Security Rule** shall mean the Security Standards for the Protection of Electronic Protected Health Information codified at 45 C.F.R. Parts 160 and 164.

ww. **SC-HIP** means South Carolina Health Information Partners, Inc., a South Carolina nonprofit corporation, the Governing Authority for SCHIEx.

xx. **SCRIPTS** means the South Carolina prescription drug monitoring program, created pursuant to the South Carolina Prescription Monitoring Act, S.C. Code Ann. 44-53-1610 et seq., which requires dispensing practitioners and pharmacists to collect and report dispensing activity of all schedule II-IV controlled substances.

yy. **Submitter** means the Participant(s), Participant Member(s) or Authorized User(s) who submit Message Content through a Message to a Recipeint for a Permitted Purpose.

zz. **System** means SCHIEx's internet-based, authenticated, peer-to-peer computer system and search engine for patient health, demographic, and related

information that assists Authorized Users in locating Data and facilitates the Adapter of Data held by multiple Health Care Organizations with disparate health information computer applications, and which allows Authorized Users to authenticate and communicate securely over an entrusted network to provide access to and to maintain the integrity of Data.

aaa. **Transact or Transaction** means to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content using the SCHIEx Performance and Service Specifications.

bbb. **Treatment** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

2. **SCHIEx Governing Authority**.

SC-HIP is the Governing Authority for SCHIEx. The Governing Authority shall have the following duties:

a. to provide policy direction and operational guidance for the SCHIEx Executive Director who shall serve at the pleasure of the Governing Authority;

b. to oversee the development, implementation, and operation of SCHIEx in compliance with all applicable state and federal requirements;

c. to establish a legal and policy framework for the operation of SCHIEx;

d. to adopt nondiscrimination and conflict of interest policies that demonstrate a commitment to open, fair, and nondiscriminatory participation in SCHIEx;

e. to develop and implement financial policies and procedures, consistent with state and federal requirements, which provide for the financial sustainability of SCHIEx;

f. to develop and implement privacy and security policies and procedures governing SCHIEx, consistent with state and federal law, including but not limited to the privacy provisions of the American Reinvestment and Recovery Act of 2009, the Privacy Act of 1974, the HIPAA Security Rule, the HIPAA Privacy Rule, the Federal Information Security Management Act of 2002, the Confidentiality of Alcohol and Drug Abuse Patient Records, and the U.S. Department of Health and Human Services Privacy and Security Framework Principles;

g. to develop the necessary agreements to facilitate the secure exchange of health information through SCHIEx and among all Participants; and

h. to encourage all applicable state agencies to participate in SCHIEx.

3. **Health Information Organizations.**

a. An HIO may choose to join SCHIEx as a Participant and may facilitate the on-boarding process and SCHIEx registration for any potential Participant Member that participates in the HIO. Nonetheless, each potential Participant Member must execute a Participation Agreement and pay the requisite SCHIEx fee as set forth in the Fee Schedule. An HIO may pay the Fee on behalf of its Participant Members so long as a Participant Member is not given access to SCHIEx until it has executed the Participation Agreement.

b. An HIO that chooses to join SCHIEx as a Participant must provide the following to SCHIEX and report any changes to the reported information within five (5) business days:

(1) a list of all current member organizations;

(2) if possible, the digital signature for each of the HIO's member organizations;

(3) name and contact information for the HIO's Privacy Officer and Site Administrator;

(4) proof that the HIO is certified to conduct business in South Carolina with the South Carolina Secretary of State's Office;

(5) proof of an active bank account in the name of the HIO's corporate entity with either a national or South Carolina bank; and

(6) proof of general liability coverage.

4. **Governing Law.**

a. Each Participant shall, at all times, comply with Applicable Law and regulations, including, but not limited to, laws and regulations protecting the confidentiality and security of Individually Identifiable Health Information and establishing certain privacy rights. Each Participant must comply with the HIPAA Privacy Rule and Security Rule even if Participant is not a Covered Entity or a Business Associate and would not otherwise be required to comply with such rules.

b. Each Participant is responsible for remaining current with all applicable laws and regulations and must ensure that it has the requisite, appropriate and necessary internal policies in place for compliance with applicable law, the HIPAA Privacy and Security Rules, the SCHIEx Participation Agreement, and the SCHIEx Policy Manual.

c. Each Participant must make a good faith effort to obtain an Individual's written acknowledgement of receipt of Notice of the Participant's participation in SCHIEx or document its efforts and failure to do so. The acknowledgement for receipt of the Notice of Privacy Practices shall comply with all applicable laws and regulations (see 45 CFR § 164.520 (c)(2)(ii)). Each Participant shall have its own policies and procedures regarding obtaining acknowledgement of an Individual's receipt of the Notice which shall be consistent with applicable laws and regulations and these SCHIEx Policies and Procedures.

d. Each Participant shall designate an employee to act as the Participant's Privacy Officer. The Privacy Officer is responsible for keeping Participant informed regarding current federal and state privacy laws and regulations, developing and implementing the Participant's own policies and procedures, conducting any internal investigations in the event of a potential breach, and for reporting all breaches.

5. **Notification of Participation in SCHIEx EXCHANGE.**

a. Each Participant in SCHIEx EXCHANGE shall develop and maintain a Notice to Individuals in either the Participant's Notice of Privacy Practices, which shall meet the content requirements set forth under the HIPAA Privacy Rule (see 45 CFR §164.520 (b)), or in a separate stand alone document that complies with applicable law and these SCHIEx Policies and Procedures.

b. Such Notice shall, at a minimum, inform Individuals regarding:

(1) Participant's participation in SCHIEx EXCHANGE;

(2) Individual information will be exchanged via SCHIEx EXCHANGE unless the Individual notifies the Participant that he or she desires to opt out of having his or her information exchanged through SCHIEx EXCHANGE, except for information required to be exchanged by federal or state law;

(3) the general range of health care information the Participant may include in and make available to other Participants through SCHIEx EXCHANGE;

(4) the exchange of information through SCHIEx EXCHANGE is governed by federal and state law;

(5) the categories of entities and Individuals who are able to access the information through SCHIEx EXCHANGE;

(6) the categories of purposes for which such information may be accessed;

(7) how the Individual can opt out of having his or her information exchanged through SCHIEx EXCHANGE and the potential effects of choosing to opt out; and

(8) how the Individual may cancel the opt out and have his or her information exchanged through SCHIEx EXCHANGE.

c. Each Participant shall have its own policies and procedures governing distribution of the Notice to Individuals, which shall be consistent with applicable laws and regulations. Participants should educate Individuals regarding Participants' participation in SCHIEx EXCHANGE, give Individuals the opportunity to ask questions regarding the same, and Notify Individuals of their right to opt out of having personal information transmitted via SCHIEx EXCHANGE. Participants should attempt to provide Individuals with a copy of the Notice prior to exchanging the Individual's information via SCHIEx EXCHANGE.

d. Participants are not required by these SCHIEx Policies and Procedures to provide separate notification of participation in SCHIEx DIRECT to Individuals. However, Participants must, at all times, comply with all applicable federal, state and local laws and regulations, including, but not limited to, laws and regulations protecting the confidentiality and security of Individually Identifiable Health Information; this obligation applies even if a Participant is not a Covered Entity or a Business Associate and would not otherwise be required to comply with such laws.

6. **Opting Out of SCHIEx.**

a. Participant must implement processes to allow an Individual to choose to opt out of having information regarding that Individual included in or made available or exchanged through SCHIEx EXCHANGE, except for certain health information required to be submitted by federal or state law. At this time, an Individual's decision to opt out of having information exchanged or made available via SCHIEx EXCHANGE is global. If an Individual opts out, no information regarding such Individual will be exchanged or made available by any Participant via SCHIEx EXCHANGE, unless Required by Law. Participants may exchange an Individual's information via SCHIEx DIRECT when allowed by applicable law, even if that Individual has opted out of having information exchanged or made available via SCHIEx EXCHANGE. Participants that utilize only SCHIEx DIRECT and the Clinical Viewer do not need to give Individuals an opportunity to opt out of SCHIEx.

b. An Individual may opt out of having his or her information included in or made available or exchanged through SCHIEx EXCHANGE by Notifying Participant, in a form and manner determined by Participant, that the Individual chooses not to have information about the Individual included in or made available through SCHIEx EXCHANGE as described in the Participant's Notice. Once an Individual has submitted a request to opt out of having his or her information included in or made available through SCHIEx EXCHANGE, the Participant shall take appropriate steps to process

the opt-out request and ensure that the Individual's information will no longer be available from Participant through SCHIEx EXCHANGE as soon as possible after receipt of the request. The Participant shall inform the Individual approximately how long it will take for the opt-out request to go into effect. Each Participant must develop and implement appropriate mechanisms to ensure no information about an Individual who has opted out shall be included in or made available through SCHIEx EXCHANGE.

c. An Individual who has opted out of having his or her information included in or made available through SCHIEx EXCHANGE may choose at a later time to have his or her information included in SCHIEx EXCHANGE. The Individual or that Individual's personal representative must request in writing, in a form or manner determined by Participant, that the Participant make the Individual's information available through SCHIEx EXCHANGE. If an Individual chooses to cancel the opt out, all available information regarding that Individual may be accessed through SCHIEx EXCHANGE.

d. Each Participant must document and maintain documentation of all Individuals' decisions to opt out of having information made available through SCHIEx EXCHANGE or to cancel the opt out and have information made available through SCHIEx EXCHANGE.

e. Participant shall not withhold care from an Individual on the basis of that Individual's decision to opt out of SCHIEx EXCHANGE and shall make every reasonable effort to avoid any adverse impact on the Individual's quality of care.

7. **Requests for and Disclosure of Information.**

a. All disclosures of health information through SCHIEx and the use of information obtained through SCHIEx shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful or discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting Participant shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing Participant.

b. A Participant, including its Participant Members and Authorized Users, shall Transact Message Content via SCHIEx only for Permitted Purposes. Information received for a Permitted Purpose must not be disclosed to any third party for any use that is not a Permitted Purpose unless required by applicable state and federal laws. Information may not be exchanged for marketing or marketing related purposes. Under no circumstances may information be exchanged for a discriminatory purpose. In the absence of a Permitted Purpose, a Participant may not Transact Message Content through SCHIEx.

c. A Participant who has access to SCRIPTS prescription drug information through SCHIEx must only request and access such information in accordance with the South Carolina Prescription Monitoring Act, S.C. Code Ann. 44-53-1610 et seq. An individual requesting and accessing SCRIPTS prescription drug information must be (i) a practitioner who possesses a DEA registration number, (ii) a pharmacist, or (iii) an "authorized delegate," who is an individual who is approved for access to the prescription monitoring program and who is directly supervised by an authorized practitioner or pharmacist; further, such individual must certify that the requested information is for the purpose of providing medical or pharmaceutical treatment to a bona fide patient.

d. Uses and disclosures of and requests for health information through SCHIEx shall comply with all SCHIEx Policies and Procedures, including, but not limited to, the SCHIEx Policies on Minimum Necessary Information and Information Subject to Special Protection, included herein.

e. Each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.

f. Each Participant disclosing health information through SCHIEx shall implement a system to document such information as may be necessary for compliance with the HIPAA Privacy Rule's accounting of disclosures requirement. Each Participant is responsible for ensuring its compliance with such requirement and may choose to provide Individuals with more information in the accounting than is required. Each requesting Participant must be able to provide information required for the disclosing Participant to comply with the HIPAA Privacy Rule's accounting of disclosures requirement.

g. Participant shall maintain an Audit log documenting who of Participant's employees and/or contractors posted and accessed the information about an Individual through SCHIEx and when such information was posted and accessed. Upon request, Participant shall provide patients with an accounting of who has posted and who has accessed information about them through SCHIEx and when such information was accessed.

8. **Information Subject to Special Protection**.

Each Participant shall determine and identify what information is subject to special protection under applicable federal, state, and/or local laws and regulations (e.g., substance abuse, mental health, and HIV) prior to disclosing any information through SCHIEx. Each Participant is responsible for complying with such laws and regulations and for appropriately designating any information requiring special protection under applicable laws as such in the Participant's electronic medical record system and, if necessary, may withhold such information from SCHIEx.

9. **Behavioral Health Information**.

a. As used herein, the term “behavioral health” refers to both mental health and substance abuse.

b. The method for exchanging health records through SCHIEx is the opt-out method. However, individual behavioral health providers may choose to use an opt-in method instead. In such cases, patients must sign an opt-in informed consent before the patients’ records may be exchanged via SCHIEx. As discussed above, the opt-out methodology is generally SCHIEx-wide, meaning that if a patient chooses to opt-out, none of the treatment records from any of his or her providers are shared through SCHIEx. However, if the behavioral health provider chooses the opt-in methodology, such consent applies only to the behavioral health records; if a patient does not otherwise opt-out of SCHIEx, his or her records from other providers may be shared via SCHIEx. The electronic health record used by the behavioral health provider must have the capability to filter out records of patients who choose not to share their information. Liability for releasing information about a patient who chooses not to participate in SCHIEx rests with the provider, not SCHIEx.

c. Substance abuse treatment records are subject to stricter federal rules than physical or mental health records. 42 CFR Part 2 requires that the patient consent indicate which specific providers can receive the treatment record, for what purpose, and when the consent terminates. Substance abuse treatment providers must always use a consent form that is compliant with 42 CFR Part 2. Treatment facilities with both mental health and substance abuse treatment programs will need a filter to signify whether a patient is in a substance abuse program covered by 42 CFR Part 2. Liability for releasing information about a patient in a 42 CFR Part 2 program rests with the provider, not SCHIEx.

10. **Minimum Necessary Information**.

a. Consistent with applicable HIPAA exceptions, each Participant shall use only the minimum amount of health Data obtained through SCHIEx as is necessary for the purpose of such use. Each Participant shall only share health Data obtained through SCHIEx with, and allow access to such Data by, those employees, agents, and contractors who need the Data in connection with a duly assigned job function or duty and who use that Data for a Permitted Purpose.

b. Consistent with applicable HIPAA exceptions, each Participant shall access only the minimum amount of an Individual’s Data through SCHIEx as is necessary for the intended Permitted Purpose of the request.

11. **Access to SCHIEx**.

a. Each Participant shall designate only those employees, staff members, agents, and contractors who have a legitimate and appropriate need to use SCHIEx as Authorized Users.

b. Each Participant shall designate an employee or agent to act as the Participant's Site Administrator. It is preferable that the Site Administrator not also serve as Participant's Privacy Officer. However, Participants with fewer than ten (10) full-time employees may utilize the same employee for both positions. The Site Administrator shall assign all log-on identifier and passcodes for Participant's employees, staff members, agents and contractors who will access SCHIEx. The Site Administrator shall Monitor SCHIEx access and verify that each employee, staff member, agent, or contractor has completed the training program required by these SCHIEx Policies and Procedures, as set forth below.

c. Each employee, staff member, agent, or contractor who will access SCHIEx shall be assigned a specific and distinct log-on identifier and private passcode required for SCHIEx access. Participant is responsible for maintaining the security of all log-on identifiers. Participants shall develop, implement, and enforce internal policies governing the use of log-on identifiers and passcodes. At a minimum, each Participant's internal policies must forbid the sharing of log-on identifiers and passcodes, include a system for conducting internal Audits to identify improper access and breaches, and allow for immediate termination of access to SCHIEx in the event of improper use or breach. No employee, staff member, agent, or contractor shall be provided with access to SCHIEx or with a log-on identifier or passcode without first having been trained on these SCHIEx Policies and Procedures, as set forth below.

d. Each Participant shall develop and implement a training program for its employees, staff members, agents, and contractors who will have access to SCHIEx, including both initial and ongoing training, to ensure compliance with federal and state laws and regulations and these SCHIEx Policies and Procedures. The training shall include a detailed review of the SCHIEx Policy Manual. Training will also include an overview of the basic technology model and operation of SCHIEx in order to ensure that Participant's staff is adequately prepared to introduce patients to SCHIEx and to respond to requests for information from Individuals. Each Participant must document and maintain documentation of training for all employees, staff members, agents, and contractors given access to SCHIEx by the Participant. Each trained employee, staff member, agent, and contractor shall sign a representation that he or she received and read the portions of the SCHIEx Policy Manual relevant to his or her responsibilities as determined by the Participant and will adhere to the SCHIEx Policy Manual**.**

12. **Enterprise Security.**

a. **General**. Each Participant shall be responsible for maintaining a secure environment that supports the operation and continued development of the SCHIEx Performance and Service Specifications. Participants shall use appropriate safeguards

to prevent use or disclosure of Message Content other than as permitted by this Agreement, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Message Content. Appropriate safeguards for Participants shall be those identified in the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, as safeguards, standards, "required" implementation specifications, and "addressable" implementation specifications to the extent that the "addressable" implementation specifications are reasonable and appropriate in the Participant's environment. If an "addressable" implementation specification is not reasonable and appropriate in the Participant's environment, then the Participant must document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate. Appropriate safeguards for Federal Participants shall be those required by Applicable Law related to information security. Each Participant shall, as appropriate under either the HIPAA Regulations, or under Applicable Law, have written privacy and security policies in place by the Participant's respective Effective Date. Participants shall also be required to comply with any SCHIEx Performance and Service Specifications or SCHIEx Policies and Procedures adopted by the Governing Authority, respectively, that define requirements and expectations for Participants with respect to enterprise security.

b. **Malicious Software**. Each Participant shall ensure that it employs security controls that meet applicable industry standards so that the information and Message Content being Transacted and any method of Transacting such information and Message Content will not introduce any viruses, worms, unauthorized cookies, trojans, malicious software, "malware," or other program, routine, subroutine, or data designed to disrupt the proper operation of a System or any part thereof or any hardware or software used by a Participant in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a System or any part thereof or any hardware, software or data used by a Participant in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this Section.

13. **Equipment and Software**. Each Participant shall be responsible for procuring, and assuring that its Authorized Users have or have access to, all equipment and software necessary for it to Transact Message Content. Each Participant shall ensure that all computers and electronic devices owned or leased by the Participant and its Authorized Users to be used to Transact Message Content are properly configured, including, but not limited to, the base workstation operating system, web browser, and internet connectivity.

14. **Reporting of Adverse Security Events and Non-Compliance**.

a. **Notification to SCHIEx**. A Participant must report any Adverse Security Event within three (3) business days of discovery of the suspected or actual Adverse

Security Event. The report must be submitted in writing to SCHIEx at reporting@schiex.org.

Participant must provide a telephone number on the Complaint Form where the Participant's Privacy Officer may be reached and must submit an online update regarding the suspected or actual Adverse Security Event to SCHIEx within two (2) business days of reporting the initial breach. Participant agrees to cooperate with SCHIEx throughout resulting breach investigation and to provide additional information to SCHIEx regarding the the Adverse Security Event as it becomes available.

This reporting requirement is in addition to any reporting requirement pursuant to applicable federal and state law. SCHIEX will report any reported actual or suspected breaches to eHealth Exchange as required by the DURSA. However, SCHIEX is not responsible for and will not report any actual or suspected breaches to any state or federal agency on behalf of a Participant. Such notifications remain the responsibility of Participant.

b. **Reporting of Other Non-Compliance**. Each Participant must report any other violation of these SCHIEx Policies and Procedures or the SCHIEx Policy Manual, including but not limited to the Interoperability Standards, failure to provide required Notice, or failure to abide by a patient's opt out request, regardless of harm, to SCHIEX within three (3) business days of discovery. Participant agrees to cooperate with SCHIEX throughout any investigation regarding suspected non-compliance and to provide additional information to SCHIEX regarding the matter as such information becomes available.

15. **Quality of Information**.

a. Each Participant is responsible for maintaining the quality and security of information entered into Participant's Electronic Medical Records (EMR) and made available to other Participants through SCHIEx. SCHIEX is not responsible for verifying or correcting any information made available by Participants through SCHIEx.

b. Each Participant shall comply with applicable federal, state and local laws and regulations regarding an Individual's right to request amendments of health information.

c. **Suspected Errors**.

(1) Should a Participant receive Data via SCHIEx DIRECT that Participant believes was intended to be sent to a different entity, Participant shall Notify the disclosing Participant as soon as possible of the suspected transmission error.

(2) Should a Participant receive Data via SCHIEx EXCHANGE or SCHIEx DIRECT that Participant believes is inacurrate or belongs to a patient other than the

patient that is the subject of the exchange, Participant shall Notify the disclosing Participant as soon as possible regarding the suspected error.

16. **Monitoring and Auditing**.

a. SCHIEx, acting through its agents and independent contractors, in order to confirm compliance with the Participation Agreement and its SCHIEx Policies and Procedures, has the right, but not the obligation to monitor and audit the Transaction of Message Content via SCHIEx. Unless prohibited by Applicable Law, Participant agrees to cooperate with SCHIEx in these monitoring and auditing activities and to provide, upon the reasonable request of SCHIEx, information in the furtherance of SCHIEx's monitoring and auditing including, but not limited to, audit logs of exchange transactions and summary reports of exchange activities, to the extent that Participant possesses such information. Each Participant represents that, through its agents, employees, and independent contractors, it shall have the ability to monitor and audit all access to and use of its System related to this Agreement, for system administration, security, and other legitimate purposes. Each Participant shall perform those auditing activities required by the Performance and Service Specifications

b. In the event that monitoring reveals a Participant's possible non-adherence to these SCHIEx Policies and Procedures, SCHIEX will attempt to mitigate the non-adherence through such measures including, but not limited to, reporting the suspected breach to the Participant and governmental authorities and issuing appropriate sanctions on the Participant as discussed below. SCHIEx must investigate any report or complaint regarding an Adverse Security Event or inappropriate access, use, or disclosure of patient information exchanged through SCHIEx or a violation of the SCHIEx Policy Manual.

c. If the Governing Authority determines that a violation has occurred or that patient information has been inappropriately accessed, used, or disclosed, the Governing Authority shall issue a letter to Participant imposing appropriate sanctions on the Participant, which may include immediate suspension or termination of Participant's access to certain SCHIEx services and/or participation in SCHIEx.

d. If the Governing Authority determines that no violation occurred, the Governing Authority shall issue a letter to Participant dismissing the alleged violation.

e. If the Governing Authority determines that the violation was minor and has been adequately addressed by the Participant, the Governing Authority shall issue a letter to the Participant setting forth its findings and recommendations, if any, to avoid future violations.

17. **Termination of Participants**.

a. **Participation Agreement**. Per the SC-HIP Participation Agreement, termination may be for Cause, Without Cause, or by Consent.

(1) Termination for Cause means the failure by the Participant to perform a material term of the Agreement. The two material terms are as follows:
   (a) Non-payment of fees, and
   (b) Material breach and failure to remedy.
(2) Termination Without Cause enables the Participant to terminate by giving sixty (60) days written notice to SC-HIP.
(3) Termination by Consent enables termination by mutual written agreement of both the Participant and SC-HIP.

b. **Non-Payment of Fees.**

(1) In the event that a participant does not pay the attributable fees associated with their participation within ninety (90) days, the Participant's access may be terminated.

c. **Material Breach and the Failure to Remedy**. If the Participant causes a material breach which is not remedied within thirty (30) days after the Participant has received notice of the Material Breach, the Participant's access shall be terminated and SC-HIP staff shall retain documentation of the notice. Notwithstanding this provision, SC-HIP may immediately suspend a Participant's access and ability to Transfer Message Content upon report of an Adverse Security Event, Breach, complaint, Material Breach, or based on other reasonable cause, such cause to be determined solely in SC-HIP's discretion. Any suspension may remain in place during an investigation into the underlying Adverse Security Event, Breach, complaint or reasonable cause and following notice to the Participant of a Material Breach prior to Participant's remedy to the Material Breach. Whether Participant has provided sufficient remedy to Material Breach is to be determined by SC-HIP and is solely within SC-HIP's discretion.

d. **Termination without Cause**. If a participant provides the sixty (60) day written notice for termination without cause, SC-HIP staff shall retain documentation of the notice and terminate the Participant's access.

e. **Termination by Consent**. If both the Participant and SC-HIP agree, in writing, to a termination of the relationship, SC-HIP staff shall terminate the Participant's access and retain documentation of the mutual agreement.

f. **Effect of Termination**. Immediately upon termination, Participant shall cease to be a Participant, and neither Participant nor its Authorized Users shall have any rights to access or use the System, as defined in the Participation Agreement, or the SCHIEx software.

g. **Exceptions**. Should an exception to this policy arise, staff will submit the exception, along with the circumstances surrounding the exception, to the Board for approval or rejection.

Revision History:

Adopted October 16, 2014
Revised October 31, 2015
Revised December 10, 2015
Revised March 16, 2017
Revised April 24, 2019
Revised September 19, 2019