**NOTICE: THIS AGREEMENT IS SUBJECT TO ARBITRATION PURSUANT TO THE SOUTH CAROLINA UNIFORM ARBITRATION ACT, SECTION 15-48-10 *ET SEQ.* OF THE CODE OF LAWS OF SOUTH CAROLINA.**

# South Carolina eHealth Alliance

# Policies and Procedures

*Version: 1.0*
*Date: April 2026*

# Table of Contents

# 1. Definitions

Terms used in this Agreement shall have the same meaning as set forth in HIPAA, unless expressly stated otherwise herein or as provided in Appendix A. A change to HIPAA which modifies any defined HIPAA term, or which alters the regulatory citation for the definition, shall be deemed incorporated into these "Policies and Procedures". Any capitalized terms in this document not otherwise defined herein have the definition given to them in the Participation Agreement.

# 2. Background

## A. Overview of SCeHA

South Carolina eHealth Alliance ("SCeHA"), the state-wide Health Information Exchange (also known as and formerly known as the South Carolina Health Information Exchange or "SCHIEx"), is a product of South Carolina Health Information Partners, Inc. ("SCHIP"), a member-based nonprofit affiliate of Health Sciences South Carolina ("HSSC"). SCeHA is built on the shared service framework of the Chesapeake Regional Information System For Our Patients, Inc.("CRISP") and is supported by CRISP Shared Services, Inc. ("CSS"). CSS additionally serves as a subcontractor to SCHIP and HSSC in connection with SCeHA. This relationship is intended for SCHIP to access CRISP's technology backbone to deliver scalable and efficient solutions, by and through SCeHA, for healthcare data exchange throughout the state of South Carolina. SCeHA integrates Data from many different sources and provides governance to ensure that Data is protected and secure. Part of this governance structure includes common "rules of the road" for persons using SCeHA Services. Specifically, each Participant must enter into the Participation Agreement, binding the Participant to these Policies and Procedures.

These Policies and Procedures contain specific terms and conditions for operation and use of the SCeHA Services, specific technical specifications information, and other terms or requirements relating to the SCeHA Services that are specified in the Participation Agreement. In the event of a conflict between a provision of the Participation Agreement and a provision of these Policies and Procedures, the provision of the Participation Agreement governs. These Policies and Procedures may be amended from time-to-time in accordance with the Participation Agreement and as set forth herein.

## B. Participating in SCeHA

To be a Participant in SCeHA, an organization must be a Covered Entity as defined under HIPAA, and may include, but not be limited to, health systems, hospitals, physician practices, insurers, Managed Care Organizations and Affordable Care Organizations. Each Covered Entity must work with the SCeHA outreach team to execute a Participation Agreement, including a Business Associate Agreement. In addition, every organization must attest whether it is covered by 42 C.F.R. Part 2. If it is, the organization must either attest to not sending any data covered by Part 2 or must sign a Qualified Services Organization Agreement Addendum. After providing the appropriate documentation, Participants work with an onboarding team to integrate with the SCeHA infrastructure and provide a list of patients with whom the Participant has a relationship. The SCeHA onboarding team also works with each Participant to update its notice of privacy practices and other documentation needed for patient education. Limited SCeHA Services may be provided to other entities that are not covered by HIPAA, as allowed by Applicable Law.

### C. Authorized Users

After onboarding, the Participant can credential Individuals from its organization as Authorized Users to directly access SCeHA Services through the SCeHA online portal or through an electronic health record ("***EHR***") system. Authorized Users may have SCeHA Services access rights at multiple Participant locations, based on their employment. If an Authorized User chooses to access the SCeHA Services via the web-based portal application made available through SCeHA, a unique username and password will be assigned to that user for each Participant with which the user is associated.

Each Participant must have an enforceable agreement with each of the Participant's Authorized Users governing the appropriate use of the SCeHA Services; see Appendix B for example text. Agreements may take the form of written policies and procedures of the Participant, as long as such policies and procedures constitute an enforceable agreement with Authorized Users. Each Participant must require that all of the Participant's Authorized Users comply with Applicable Laws, the Participation Agreement, and these SCeHA Policies and Procedures. If an Authorized User is in violation of any of these terms, the sponsoring Participant must immediately notify SCHIP, and SCHIP may suspend or terminate the Authorized User's access to the SCeHA Services as necessary.

## 3. Corporate Structure and Governance

### A. Corporate Governance

A board of directors of SCHIP (the "***Board***") oversees SCeHA and provides guidance and input on certain key decisions during the development and operations of the SCeHA Services. Decisions made by the Board are final.

The Board has the authority to form additional advisory committees in its discretion. The general responsibilities of each committee shall be defined by their respective charters or pursuant to the Bylaws of SCHIP. Copies of the Bylaws and any of these charters will be made available to Participant upon request. The Board appoints individuals to each committee, selecting from among those who have been identified by or made known to SCHIP who are deemed qualified for the particular committee and are willing to serve. The Board aims for the most capable team possible, while also seeking to ensure geographic and organizational diversity, and after consultation with state officials.

### B. Data Governance

Uses for the Data are governed by the Permitted Purposes in the Participation Agreement, which are further explained and authorized, as necessary, through use cases. The Board is responsible for approving any new use cases, all of which are posted on the SCeHA website. In addition, the Board may provide advice and guidance on uses of the Data that may raise specific privacy concerns. SCeHA may not use or exchange any Data outside of the Agreement or other agreements governing the Data.

## 4. Permitted Purposes for Data Use

### A. Permitted Purposes

Participants and Authorized Users may access and use Data through SCeHA Services for Permitted Purposes. "Permitted Purpose" shall mean one of the following reasons for which Participants, Participant Members, and Authorized Users may legitimately exchange Data through SCeHA. Permitted Purposes for SCeHA 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 SCeHA 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, 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 1-69 of these definitions 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;

g. A Public Purpose.

SCeHA may add Permitted Purposes according to the process set forth in the Participation Agreement.

Permitted Purposes may be further specified through use cases, which can be found on the SCeHA Website at www.SCeHA.org. The use cases are approved and amended by the Board before their incorporation into a Permitted Purpose.

With the approval of the Board, specific use cases may be extended to other entities, upon a finding that such an extension is in furtherance of the mission of SCeHA, that entry into a full Participation Agreement is not possible or practical, and provided that the entity will be required to enter into a written agreement with SCHIP that protects the interests of SCHIP, SCeHA and its Participants, the integrity of the SCeHA Services, and the appropriate use of the information to be provided to the entity.

SCHIP may allow access or otherwise release Data from the SCeHA Services for public health reporting or in other civil, criminal, or crisis-related matters where compelled to provide that Data by a lawful order. Each request for Data from non-Participants will be independently vetted to ensure the request is legal and appropriate. SCHIP will not release any Protected Health Information to anyone for commercial, private, or other reasons that are not related to the Permitted Purposes.

Participant shall not use any SCeHA Service or permit any Authorized User to use SCeHA Services to conduct any business or activity, or solicit the performance of any activity, which is prohibited by or would violate any Applicable Law, or for purposes that may create civil or criminal liability in Participant or SCHIP, including but not limited to: (i) uses which are defamatory, deceptive, obscene, or otherwise inappropriate; (ii) uses that violate or infringe upon the rights of any other Individual, such as unauthorized distribution of copyrighted material; (iii) “spamming,” sending unsolicited bulk e-mail or other messages or sending unsolicited advertising or similar conduct; (iv) threats to or harassment of another; (v) knowingly sending any virus, worm, or other harmful component; (vi) attempting to gain unauthorized access to SCeHA or any computer system of any Participant or SCHIP; (vii) impersonating another person or other misrepresentation of source; and (viii) any action in violation of HIPAA or state laws relating to the privacy or security of an Individual’s medical information.

Participant or Authorized Users may not access or use the Data or any Confidential Information of another party received via the SCeHA Services to compare patient volumes or practice patterns, unless Participant enters into a separate data sharing agreement with the other Participant that is the source of the Data or Confidential Information. Participants agree to take any action required to assure antitrust law compliance at all times. Notwithstanding anything to the contrary, all activities described in this Agreement are to be limited by and performed only in strict compliance with all federal and South Carolina antitrust laws, including, but not limited to, the Sherman Antitrust Act, 15 U.S.C. §§ 1-7 (1890).

## B. Use Cases

For all access and use of Data other than the Permitted Purposes, the use and purpose must be further explained and specified through use cases before the Data may be accessed or used through the SCeHA

Services in that manner. The use cases are approved by the Board, which may create specialized subcommittees to review certain use cases. All approved use cases are available on the SCeHA website.

### C. Sensitive Data and Consent Management

If Applicable Law protects Data such that it cannot be released without the affirmative consent of the Individual (e.g., Data covered by 42 C.F.R. Part 2), the Data may not be used for any of the Permitted Purposes unless and until an authorized person enters the required consent of the Individual. Data that does not require affirmative consent or authorization under Applicable Law may be accessed for any Permitted Purpose.

Data contributors of Participants must refrain from sending certain sensitive health information, including but not limited to, substance use disorder treatment and self-pay information that may be restricted by Applicable Law, unless a *separate* written agreement has been executed with SCHIP to share sensitive Data in accordance with Applicable Law. Participants are responsible for ensuring that their disclosure of information to SCeHA complies with all Applicable Law. If a Participant believes it holds information that is subject to special protection under Applicable Law, the Participant must work with SCHIP to determine: (i) whether the appropriate legal framework is in place for the disclosure to SCeHA; and (ii) whether it is technologically feasible for SCHIP to manage access to and further disclosure of such information through the SCeHA Services in a manner compliant with Applicable Law. If either of the foregoing are not in place and/or feasible, the Participant must not share such information with SCeHA and/or through the SCeHA Services.

## 5. Accessing SCeHA

A Participant may contribute and/or consume Data either via the SCeHA Services or through a third-party EHR. The hardware and software requirements for access/use of the SCeHA Services depend on the means an organization is using to contribute/consume Data and are the responsibility of the Participant.

Authorized Users can access the SCeHA Services in two ways. First, Authorized Users may access via the online portal.

Additionally, Authorized Users can also access the SCeHA Services through their EHR. SCeHA connects to and exchanges Data with many EHR vendors; users must single sign-on to their EHR service to also authenticate to SCeHA and access Data through the SCeHA Services. Unlike access through the online portal, Participants monitor the Authorized Users' access and authentication without additional SCeHA requirements. Single sign-on access to the SCeHA Services leverages the industry standards Substitutable Medical Apps and Reusable Technology ("SMART") on Fast Healthcare Interoperability Resources ("FHIR") and Security Assertion Markup Language ("SAML") 2.0. All launches require information identifying the unique user and organization launching the service in addition to specific patient identifiers.

## 6. Participants' Responsibilities

### A. Onboarding and Testing

Participants must complete testing and other onboarding activities prior to going live with connectivity to SCeHA. These testing and onboarding activities are tailored to the type of Data being provided and accessed and typically include submission of a patient panel. SCHIP will communicate these requirements during the onboarding process. Data validation should be completed by comparing the Data in SCeHA's System to that in the Participant's source system. SCHIP will provide guidance on testing, but it is the Participant's responsibility to execute a complete test plan in accordance with Participant's own testing

policies and procedures. Following successful completion of Participant testing, Participants must provide confirmation to SCHIP that they are ready to go live. Participants should notify SCHIP prior to any system changes or updates.

## B. Compliance with Applicable Law

### i. Federal, State, and Local Privacy Laws

All Participants must, and must require Authorized Users to, comply with Applicable Law, including federal, state, and local privacy laws. As noted above, Participants are responsible for complying with Applicable Laws, gaining necessary consent or authorization, and filtering information, as necessary. If a Participant believes it holds information that the Participant is prohibited by Applicable Law from sharing, that information must not be shared with or through SCeHA.

### ii. Federal Information Blocking Prohibition

The 21st Century Cures Act and its implementing regulations prohibit certain individuals and entities from engaging in "information blocking." Information blocking is any practice - an action or inaction - by an "actor" that interferes with access, exchange, or use of Electronic Health Information unless that practice is required by applicable law or satisfies a public policy-based exception set forth in the regulations. Actors, under the information blocking regulations, include:

1. Healthcare providers;
2. Health Information Networks / Health Information Exchanges ("HIN"s/"HIE"s); and
3. Developers or offerors of Certified Health Information Technology.

Compliance with the prohibition against information blocking is consistent with SCeHA's mission and purpose as a Health Information Exchange.

Part of SCeHA's compliance obligations, as an HIE, include requiring that Participants meeting the definition of an actor also agree to comply with the prohibition against information blocking in their use of SCeHA. For actor-Participants, the information blocking regulations are Applicable Law, and failure to comply with those regulations would constitute a breach of the Participation Agreement. SCHIP will investigate allegations of information blocking by a Participant that involve the Participant's use (or non-use) of the HIE and will take appropriate action. All Participants must reasonably cooperate with such investigations, even if the Participant intends to assert that it is not an actor under the information blocking regulations.

More information regarding the information blocking regulations is available in the *Information Blocking Frequently Asked Questions* that have been developed by the Office of the National Coordinator for Health Information Technology ("***ONC***"), available here.

## C. Disputes

Participants agree first to enter into good faith negotiations at an executive level, between or among themselves or involving SCHIP (as the case may be), to resolve any controversy, claim, or dispute arising out of or relating to the Participation Agreement or the Policy Manual, including these Policies and Procedures ("***Dispute***"). Therefore, Participants will resolve disputes using the following process.

### i. Referral to Executives

In the event that an executive level meeting fails to resolve the Dispute within thirty (30) days after the first meeting of executives, Participants shall seek to resolve the Dispute pursuant to nonbinding mediation.

### ii. Mediation

In the event that the Dispute is not resolved within thirty (30) calendar days of the appointment of a neutral mediator, unless any Participant requests an extension for a reasonable period of time, any Participant may seek to resolve the Dispute in accordance with Section 6(c)(iii) below.

### iii. Nonbinding Arbitration

In the event that the Dispute is not resolved pursuant to Section 6(c)(ii), Participants agree that any Dispute arising out of the Participation Agreement (other than an action or proceeding for injunctive or other equitable relief), shall be resolved by a firm or individual (mutually acceptable to all parties involved), who is a subject matter expert recognized in the field of the Dispute (the "Arbitrator"). The arbitration shall be conducted in Columbia, South Carolina in accordance with the American Health Lawyers Association Alternative Dispute Resolution Service Rules of Procedure for Arbitration then in effect. Participants acknowledge and agree, however, that the Arbitrator is empowered, within his, her, its, or their determination, to direct SCHIP to suspend access to and use of SCeHA by any Participant and/ or any Authorized Users. In the event that the Arbitrator determines that an appropriate remedy to a Dispute includes the suspension of any Participant and/ or any of its Authorized Users, SCHIP shall comply with such determination.

### iv. Further Resolution

Following the determination of an Arbitrator, Participants understand and agree that any party to the Participation Agreement may appeal the decision of the Arbitrator by instituting proceedings within a South Carolina court of competent jurisdiction. Pending final resolution on the matter in Dispute, the parties shall proceed diligently with the performance of their respective responsibilities and will comply with their respective obligations under the Participation Agreement, including any determination of the Arbitrator, as applicable.

### v. Immediate Injunctive Relief

The dispute resolution process set forth above does not act to forestall any Participant or SCHIP from seeking immediate injunctive relief based on a good-faith determination that another Participant's actions or inactions are likely to cause irreparable harm to SCHIP or to the Participant seeking such equitable relief. Provided, however, that a Participant seeking immediate injunctive relief against another Participant must inform the CEO within three (3) business days of: (i) filing for such relief; and (ii) the outcome of the action. No dispute that is pending before a court of competent jurisdiction will be subject to this dispute resolution process during such pendency.

## D. Procedures for Participant Non-Compliance

In accordance with the Participation Agreement, each Participant must implement procedures to mitigate and deter misuse of SCeHA Services and Data and to issue appropriate sanctions to hold Authorized Users responsible for misuse of Data obtained when accessing Protected Health Information through the SCeHA Services. As applicable, procedures in place for the appropriate use of other health information systems may be leveraged for the use of Data through the SCeHA Services.

### E. Data Completeness

Participants, by electing to receive Data through the SCeHA Services, authorize SCeHA to transmit results, reports, and other patient information directly from Participants' ancillary providers, such as clinical laboratories and radiology centers. Participants are responsible for the accuracy, quality, and completeness of the Data provided using the SCeHA Services. Participants should transmit Data understanding that other Participants may use these Data for important decisions, including decision making for the treatment of patients, or related payment thereof. If Participants discover that they have submitted inaccurate or incomplete Data, they should immediately notify SCHIP and cooperate with SCHIP for appropriate remediation. Likewise, Participants must understand that SCHIP cannot guarantee that the Data submitted to SCeHA and made available through the SCeHA Services are complete and/or free from error. SCHIP has no role in verifying the accuracy of any Messages, nor verifying whether a Participant or Authorized User is authorized to send, use, or disclose particular Data and/or secure Messages using the Licensed Service.

### F. Fees

SCHIP charges appropriate and reasonable fees to Participants for use of the SCeHA Services. The fees reflect the necessary and reasonable costs to provide the SCeHA Services, including technical infrastructure and operational costs. Fees may increase yearly to cover operating costs and may vary among different Participants depending on a variety of factors.

## 7. Participants' Responsibilities for the Authorized Users

### A. Participant Access Policies for Authorized Users

All Participants are required to develop, or have in place, written requirements that govern Participant's and Authorized Users' access to information Systems and use of Protected Health Information. Such policies must be consistent with the Permitted Purposes in the Policy Manual and must be made available to SCHIP upon request. Participants must appoint an authorized individual to implement and ensure compliance with all policies related to SCeHA Authorized Users. The authorized individual will be responsible for implementing a policy that appropriately grants Authorized Users access to clinical Data on behalf of the Participant and its clinicians and other appropriate individuals. This authorized individual may also act as the designated point of contact for SCeHA correspondence and user verification and updates as described above.

Participants are responsible for promptly informing SCHIP when the job status or role of an Authorized User within their organization has changed and affects the Authorized User's access rights to the SCeHA Services. If an Authorized User is being terminated from a Participant, the Participant must inform SCHIP of this termination within forty-eight (48) hours (excluding weekends and holidays), and prior to actual termination if at all possible. SCHIP will terminate the Authorized User's account upon notification of termination of employment from the respective Participant. Participants accessing the SCeHA Services through third-party EHRs, via Standard-Setting Organization/Security Assertion Markup Language ("SSO/SAML"), will be responsible for terminating access through that EHR for the terminated Authorized User prior to or at the time of termination. However, Participants must still notify SCHIP within 48 hours of the termination, so that SCHIP can terminate access to other SCeHA tools and services that are not accessed via SSO/SAML.

### B. Minimum Necessary and Role-Based Access

Authorized Users agree to view, use, and/or disclose the minimum amount of information necessary for the purpose of such use. Authorized Users should only have access to the minimum amount of information required to perform their job function. Minimum necessary does not, however, apply to use of Data for Treatment or other purposes Required By Law. It is the Participant's obligation to ensure the appropriate use of SCeHA Services by Participant and its Authorized Users and Authorized Users.

### C. Misuse of System or Data

Health information available through SCeHA is to be accessed, viewed, and used only by SCeHA Participants and Authorized Users who have been authorized to do so and only for Permitted Purposes. SCeHA uses a privacy tool for additional monitoring of all user activities around Protected Health Information access to ensure all provisioned accounts are being used appropriately and to protect the privacy of personal health information; however, it is ultimately the Participant's obligation to ensure the appropriate use of SCeHA Services by Participant and its Authorized Users. Any misuse of Protected Health Information in connection with SCeHA Services must be reported by Participant to SCHIP as soon as discovered. Potential health information misuse will be investigated. SCHIP will notify the privacy and / or security officers of all impacted parties at the conclusion of such investigations, if it is determined that a misuse of Protected Health Information has occurred. As appropriate, SCHIP will also take actions necessary to remedy the misuse of Data and/or to protect against further misuse. These actions may include, but are not limited to, suspension and/or termination of use by a Participant or Authorized User(s).

### D. Procedures for User Non-Compliance

In accordance with the Participation Agreement, each Participant must implement procedures to mitigate and deter misuse and issue appropriate sanctions to hold its Authorized Users responsible for misuse of Data obtained when accessing Protected Health Information through the SCeHA Services. As applicable, procedures in place for the appropriate use of other health information systems may be leveraged for the use of Data through the SCeHA Services.

### E. Training

SCHIP will make training resources available through the SCeHA website, in addition to other training materials, as appropriate. Participants will be responsible for training their Authorized Users on Data consumption in accordance with the Policy Manual, including through the dissemination of any necessary training provided by SCHIP and the development and implementation of any additional, internal training needed to ensure appropriate use. If additional training is necessary as a result of system updates, SCHIP will provide training through the website and inform Participants of the changes, and each Participant will then be responsible for training all of its Authorized Users.

### F. Usernames and Passwords

SCHIP utilizes security-industry best practices for authenticating and authorizing user access to SCeHA Services. Participants must ensure, in accordance with the Participation Agreement and associated Business Associate Agreement, that each Authorized User has the appropriate access and is provisioned accordingly.

SCeHA password requirements may differ across the SCeHA Services, depending upon the unique characteristics of the tool/service and the Data made available therein. SCHIP will communicate the

requirements for each tool as needed. Authorized User passwords will expire every ninety (90) days, requiring that each Authorized User create a new password at that time. Password history settings are enforced.

Authorized Users will be able to reset their own password during initial login for the online portal. A user will be locked out of the system after five (5) consecutive failed log-in attempts. An Authorized User must email Support@SCeHA.org or call the SCeHA support desk at 1-844-864-5100 for assistance if their account is locked. The support desk will verify the Authorized User's information and assist them in regaining access. Authorized User accounts are automatically locked after ninety (90) consecutive days of inactivity. Authorized Users not using Standard-Setting Organization must have their accounts verified every ninety (90) days by the authorized administrator of the Participant.

### G. HIE Administrators

Participants that are acting as consumers of Data are required to provide at least one, but preferably two, points of contact as "HIE Administrators" for the SCeHA Services. The HIE Administrators are responsible for the maintenance of user profiles, including providing all necessary information to SCHIP for adding users, deleting users, and assigning or changing user roles. The HIE Administrators should notify SCHIP if a user's employment at the organization has been terminated or if such user's functional role has changed, in accordance with these Policies and Procedures. This notification may be done either using the self-service HIE Admin Tool (recommended) or by email to Support@SCeHA.org. HIE Administrators are also responsible for attesting to user identity verification and checking that users have completed all necessary policy training prior to obtaining access to the SCeHA Services, as well as for monitoring the general use and operations of the SCeHA Services within their organization.

### H. Auditing

All Participants are required to monitor and audit access to and use of their information technology systems in connection with SCeHA Services and in accordance with their usual practices based on accepted healthcare industry standards and Applicable Law. In the event SCHIP wishes to exercise its right to audit the Participant, Participant will provide SCHIP with monitoring and access records upon request.

SCHIP regularly reviews Authorized Users' access to and use of the SCeHA Services and may take action against any misuse by an Authorized User, including suspension and/or termination of SCeHA Services access. SCHIP uses a privacy tool for additional monitoring of all user activities around access to Protected Health Information to ensure all provisioned accounts are being used appropriately and to protect the privacy and security of Protected Health Information; however, it is ultimately the Participant's obligation to ensure the appropriate use of SCeHA Services by the Participant and its Authorized Users.

## 8. System Operations

### A. Standards

SCHIP aims to support and maintain the SCeHA Services in a standards-compliant manner and, when possible and appropriate, will use best practices and generally accepted standards that are recognized by state, federal, and/or industry authorities.

### B. Availability and Network Monitoring

SCeHA Services are Monitored continuously by SCHIP and/or third-party vendors. SCHIP and its vendors maintain agreements that provide for at least 99.7% uptime per calendar month, not including scheduled

downtime. SCHIP commits to 99.9% of messages being delivered within twenty-four (24) hours of receipt of an admission, discharge, or transfer message from the supplying Participant. For each calendar year, scheduled hardware, software, and communications maintenance will not exceed an average of eight (8) hours in total per calendar month. All scheduled maintenance will be carried out on dates and at times authorized by SCHIP with at least three (3) business days' notice provided by SCHIP or the applicable vendor to all Participants via e-mail or other electronic method, such as the website. In the event of unexpected downtime, SCHIP will provide notifications to Participants via e-mail or other electronic method, such as the SCeHA Portal or SCeHA website.

### C. Maintenance

Participants will be required to provide support contact information to SCHIP. Participant support staff will be expected to assist with matters related to on-going training, master patient index administration, Data quality, system upgrades and downtime, and privacy and security matters.

### D. Support

With the exception of help desk staffing, SCeHA is closed on the following holidays:

- New Year's Day
- Martin Luther King Jr. Day
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Thanksgiving Day
- Christmas Day

### E. Implementation Support

SCHIP makes available the following implementation support services to the Participant:

- Establish environments (test and production) for secure transactions;
- Configure environments based on these Policies and Procedures regarding privacy, security, and consent;
- Conduct planning and decision sessions;
- Jointly document transaction types;
- Jointly document Data conversion and mapping requirements;
- Establish real-time notifications, if applicable;
- Test and validate real-time notification, if applicable;
- Establish batch transaction, if applicable;
- Test and validate batch transactions, if applicable; and
- Ensure access to SCeHA Services as appropriate.

### F. Operations Support

SCHIP makes available the following operational support services to the Participant:

- At least daily backups of the production environment;
- Transaction logs of all database updates that occur between daily backups;
- Periodic performance management;

- Disaster recovery using an alternate recovery site, as needed in the event of a catastrophic failure of the primary production site location;
- Maintain uptime of services;
- Maintain datasets with Data supplied by SCeHA or Participant; and
- Support Participant's periodic reconciliation of notification and claims-based encounter information.

### G. User and Technical Support

SCHIP offers Participants technical support to respond to technical problems, including support for test and production environments. SCeHA technical support personnel can be reached at support@SCeHA.org or 1-844-864-5100. SCeHA support uses a ticket logging system that documents and enables triage based on issue severity. Depending on the nature of the issue, technical problems may be dealt with directly by SCHIP staff or, in certain situations, may be raised to the attention of a vendor. For all reported problems, SCHIP will work to find a resolution in a timely manner and update Participants of actions taken, as appropriate. The help desk provides support twenty-four (24) hours a day, seven (7) days a week, including weekends and holidays.

# 9. Patient Rights and Individual Access

### A. Opting Out of SCeHA

Unless otherwise required by Applicable Law, SCeHA's default patient consent policy is an opt-out model. A patient must proactively, and explicitly, register an opt-out with SCeHA for their Data not to be exchanged through SCeHA except as Required By Law. Opting out means that a patient's health information can no longer be returned as the result of a Query-Retrieve or sent as an encounter notification, unless exceptions in Applicable Law apply. For example, opt out does **not** limit point-to-point secure messaging (results and referrals); if a primary care physician orders a lab test from a national laboratory, the result for that order will still be electronically delivered to the ordering provider but the result will not be available to other physicians who query the exchange.

Patient opt out is centrally managed by SCHIP. However, it is the Participant's responsibility to adequately educate patients on the opt-out process and to ensure that its Notice of Privacy Practices is updated accordingly. Patients can opt out by completing the online form (https://connect.sceha.org/OptoutForm) or calling the toll-free number (1-844-864-5100). There may be a period of up to five (5) business days after SCeHA's receipt before the opt out is effective in the System, meaning that patient Data may be available for query during this interim time after the opt-out has been submitted. Patients are allowed to opt back into SCeHA at any time, but patient Data may have been deleted at the time the opt out went into effect.

The foregoing opt-out right shall also apply to External HIEs. SCHIP shall not respond to queries by External HIEs with data for Individuals who have opted out of SCeHA. SCeHA users will not be able to query External HIEs for any individual who have opt-ed out of SCeHA. SCHIP shall not be responsible for the Individual's opt-out status for External HIEs other than as aforementioned. SCHIP will provide notice to Individuals on the SCeHA website of SCeHA participation in External HIEs and of the corresponding opt-out process for each.

### B. Accountings of Disclosures

Patients may request an accounting of disclosures from SCHIP that shows Participating Users' access to and disclosure of the patient's information through the SCeHA Services. Patients may obtain an accounting twice per year before being charged a reasonable, cost-based fee for preparing and providing an accounting of disclosure. Patients or Guardians can request an account of disclosure by completing the online form at https://sceha.org/patients.php.

### C. Secondary Use of Data

SCHIP will not, and will also contractually require Exchange Technology Providers and Licensed Technology Providers or any other agent or contractor of SCHIP with access on other than an incidental basis to Data to not, use or disclose Data provided to the HIE by HIE Participants or available from the HIE about HIE Authorized Users except as may be required by Applicable Law or deidentify Data in order to engage for a Secondary Use (as defined below) or provide the Data or information derived from the Data to any other person or entity, including a related entity or a third party, for the recipient's Secondary Use, even if, in all cases, the Secondary Use is otherwise permitted by Applicable Law, unless as to a Secondary Use permitted by Applicable law, the permitted Secondary Use has been approved by the Advisory Board through the process and under the standards set forth herein. A Secondary Use is the use of the Data or the extraction of information from the Data for analytic, predictive, or other business purposes, including but not limited to Monitoring or analysis of practice or utilization patterns of Participant or Authorized Users.

## 10. Interstate Data Exchange

### A. External HIEs

One of the main goals of SCeHA is to ensure that health Data are available where needed for clinicians and patients to make the best decisions, no matter where in the United States and territories a patient receives care. Therefore, SCHIP has direct agreements with several neighboring states for robust Data sharing in areas where patients in South Carolina are most likely to seek care. In addition, SCeHA participates in several national networks; these national networks electronically connect HIEs and more localized Health Information Networks (HINs) throughout the country. The national networks provide a common framework for technology, as well as privacy and security standards. Currently, SCeHA participates in the following national networks and interoperability frameworks:

- eHealth Exchange
- CommonWell
- Carequality

Each of these networks and frameworks has its own governing body, rules, and legal agreements, but how they work conceptually is the same.

Subject to the approval by the Board, SCHIP may enter into agreements with External HIEs for the use of the HIE and Participant's and Other Participants' Data for purposes of the External HIE (such as making and responding to queries the System provided or required by the particular External HIE provided that: (i) such an agreement is permitted under or is consistent with the Applicable Law; and (ii) SCHIP provides Notice to Participant of the material terms and conditions of participation with an External HIE; (iii) such an agreement requires the External HIE to comply with privacy and security requirements that are the same as, or no less stringent than, the requirements that apply to SCeHA in the Agreement; and (iv) such

an agreement requires the External HIE to maintain insurance coverage of the same types and with minimum limits and standards that are equivalent to, or no less than, those required to be carried by SCHIP as set forth in the Agreement. SCHIP will also either make the External HIE Materials available to Participant with the Notice described in clause (ii) above of the preceding sentence or advise Participant of how to obtain copies of the External HIE Materials and Participant is responsible for reviewing the External HIE Materials.

Requirements as to a Participant's use of the HIE in the Agreement shall, unless provided otherwise, also govern the Participant's use of External HIEs with which SCeHA participates, and participants in an External HIE shall have the same rights as Other Participants as relates to the use of the HIE, including access to Data.

### B. National Networks and TEFCA

The Trusted Exchange Framework and Common Agreement ("TEFCA") is a government-endorsed framework for the nation-wide exchange of health information that is intended to further connect existing national networks. A goal of TEFCA is to make sure all the national networks are connected so that no one needs to connect to multiple networks. SCeHA utilizes CSS, which participates in TEFCA through the eHealth Exchange QHIN, serving as an on-ramp for its affiliated HIE participants to access the nationwide exchange.

## 11. Reporting Privacy and Security Concerns

In the event that a Participant determines that any Data transmitted through SCeHA Services have been requested, accessed, used, or disclosed by the Participant or an Authorized User in a manner that does not comply with Applicable Law and/or the provisions of the Participation Agreement, Business Associate Agreement, and/or the Policies and Procedures, the Participant must notify SCHIP of the event within two (2) business days of the determination. Notification must include a detailed summary of the relevant facts. The notification will be treated as Confidential Information, except as otherwise required pursuant to Applicable Law or as used or disclosed by SCHIP in connection with the exercise of SCHIP's rights and/or obligations under the Participation Agreement to defend its actions in any process or proceeding begun by or involving the Participant or under Applicable Law. The Participant must cooperate with SCHIP as to any further investigation or responsive action reasonably requested or taken by SCHIP to respond to the event.

In the event SCHIP determines that any Participant Data transmitted through SCeHA Services has been requested, accessed, used, or disclosed by SCHIP in a manner that does not comply with Applicable Law and/or the provisions of the Participation Agreement and that such event constitutes a Breach under HIPAA, SCHIP will comply with the provisions of the Business Associate Agreement.

## 12. Requests for Data

### A. Data Extracts

Along with the Data provided through the SCeHA Services, Participants may ask for extracts of Data, provided the Participants have the appropriate access rights. A cost-based fee for compiling these Data may be assessed based on the necessary and reasonable costs to provide the Data, including technical infrastructure and operational costs.

### B. Business Associates of Covered Entities

Participants may also request Data be sent to their Business Associates by completing a form attesting to the relationship with the Business Associate and providing a point of contact. A cost-based fee for sending Data or establishing a Data feed to a Business Associate may be assessed based on the necessary and reasonable costs to provide the Data or establishing a Data feed, including technical infrastructure and operational costs. SCHIP may also require the Business Associate to enter into an agreement regarding the type of connection and/or appropriate Data use.

## 13. Termination of Participation and Return or Destruction of Data

If a Participant terminates access to the SCeHA Services in accordance with the Participation Agreement, SCHIP will disable that Participant's Data feeds and terminate the Participant's ability to access the SCeHA Services in accordance with the Participation Agreement. Data that have been incorporated into a Participant's system of records prior to Participant termination may be retained as permitted by and in accordance with Applicable Law. Additionally, SCHIP or Participant may retain one copy of the other's Confidential Information to the extent reasonably necessary to document matters relating to the Participation Agreement for legal or insurance reasons or for similar purposes, provided that the restrictions on Confidential Information in the Participation Agreement section continue to apply to the retained copy. SCHIP retains Data consistent with Applicable Law and each Business Associate Agreement to which SCHIP has entered with a Participant. Among other things, this retention allows SCHIP to maintain an auditable history of each transaction through the SCeHA Services.

## 14. Policies and Procedures Amendment Process

SCHIP reserves the right to make amendments to these Policies and Procedures, as permitted under the Participation Agreement. Notice of amendments may be provided by posting the amendment, along with its effective date, on the SCeHA website at www.SCeHA.org, or through other means permitted under the Participation Agreement.

# Appendix A – Definitions

1. "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.

2. "Agreement" shall mean the Participation Agreement, Policies and Procedures, and Business Associate Agreement, which shall be set forth on the SCeHA website, www. SCeHA.org.

3. "Applicable Law" shall mean the federal, state, and local laws, rules, policies, regulations, and standards adopted by administrative agencies that are applicable to either SCHIP or Participant or a party's rights and obligations under the Agreement, including, without limitation, laws, rules, and regulations applicable to the confidentiality of patient records and the protected information.

4. "Audit" shall mean a review and examination of records (including log or other records generated by or available through an information system), and/or activities to ensure compliance with the Agreement and the Policy Manual and to ensure accuracy of the data transmission and conversion of data by the Adapter. The audit process can be manual, automated, or a combination of both.

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

6. "Authorized User" as to the HIE and SCeHA Services shall mean those health care providers and other employees, staff, professional or medical staff, contracted medical providers, agents, or other workforce members of Participant and Other Participants who have been authorized by Participant or Other Participant to utilize the HIE for a Permitted Purpose through Participant's System or through user interfaces made available by SCHIP and who have at the request of Participant or as otherwise provided in the Policies and Procedures, been assigned a username and password by SCHIP pursuant to the Agreement. An Authorized User shall also mean 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. An Authorized User may act as either a Submitter, Recipient, or both when Transacting Message Content. 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. SCHIP will establish, through its Policies and Procedures, terms and conditions applicable to Authorized Users that are members of the professional staff of those Participants and Other Participants that have organized professional

staffs. Unless otherwise specified, Authorized Users shall only be natural persons and shall not be other legal or operating entities or affiliates or subsidiaries of Participant except as may be provided in the Policies and Procedures. References to Participant will be deemed to include a reference to the Participant's Authorized Users unless the context requires otherwise.

7. “CEO” means the chief executive officer of SCHIP.

8. “Common HIE Resources” shall mean the technologies utilized by SCeHA from time-to-time withthe approval of the Board and the software, portal, platform, interfaces, or other electronic medium controlled by SCHIP through which SCHIP makes SCeHA Services available to Participant under the Agreement. SCHIP will keep a record of Common HIE Resources.

9. “Confidential Information” shall mean information that relates to a party’s past, present, or future business activities, finances, practices, protocols, products, services, information, content, technical knowledge, information obtained pursuant to the Agreement, which is otherwise protectable by patent, copyright, or trade secret, which has been designated in writing as confidential when disclosed to the other party to the Agreement, or which is, by its nature, something that would reasonably be understood to be confidential by a recipient familiar with the health care industry. Notwithstanding the foregoing, the term “Confidential Information” does not include any information which: (i) was already known to the receiving party; (ii) was generally available to the public prior to disclosure to the receiving party; (iii) was developed by the receiving party independently of disclosure by the disclosing party; or (iv) was disclosed to the receiving party by a third party without any obligation of confidentiality or restriction on use. Confidential Information also does not include Data, which is subject to Applicable Law and to the separate provisions of the Agreement specific to Data, including the Business Associate Agreement.

10. “Data” shall mean “Electronic Health Information” as defined by 42 C.F.R. 171.102 and other Protected Health Information, Individually Identifiable Health Information, De-Identified PHI, or Limited Data Sets, all as defined in the HIPAA Regulations, and metadata, that is requested, disclosed, stored, or is transmitted or available from Participants, Other Participants, or Data Sources for transmission through the HIE in accordance with the provisions of this Agreement and the requirements of Applicable Law, including without limitation, HIPAA and state medical privacy laws.

11. “DURSA” means the Second 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.

12. “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.

13. “Electronic Protected Health Information” or (“EPHI”) has the same meaning as the term "electronic protected health information" in 45 C.F.R. §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.

14. “Exchange Technology Provider” shall mean an entity that provides Common HIE Resources for the HIE to SCHIP or an entity that provides items or services used by SCHIP in connection with the HIE.

15. “External HIE” shall mean other entities and services that provide health information exchanges that are not part of the HIE, including national networks and regional health information exchange organizations, which provide for participation by SCHIP, and through SCeHA, SCeHA Participant and Other Participants, in the exchange of health information on an intrastate, interstate, regional, or national basis directly or through participation with a third party organization or entity, including but not limited to so-called national exchanges and vendors of Electronic Health Records.

16. “External HIE Materials” shall mean agreements, descriptions, specifications, policies and procedures, or other materials made available by External HIEs for their Participants, which may include material required for compliance with a federal government developed trusted exchange framework.

17. “Governing Authority” means South Carolina Health Information Partners, Inc., a South Carolina nonprofit corporation, which is responsible for administering SCeHA and fulfilling the roles and responsibilities described herein.

18. “Health Care Operations” has the meaning set forth in 45 C.F.R. §164.501 of the HIPAA Regulations.

19. “Health Care Provider” has the meaning set forth in 45 C.F.R. §160.103 of the HIPAA Regulations.

20. “Health Information Exchange” or “HIE” shall mean the Common HIE Resources and infrastructure made available to Participants by SCeHA for Permitted Purposes, subject to the terms of the Agreement.

21. “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.

22. "HIPAA" shall mean the Health Information Portability and Accountability Act of 1996, specifically including the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164) as amended by the Health Information Technology for Economic and Clinical Health Act, enacted as Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009, including regulations published as the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (the "Omnibus HITECH Rule"). Vol. 78 Federal Register 17 (January 25, 2013) and as any further amendments, modification, or renumbering which occurs or takes effect during the term of the Agreement.

23. "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.

24. "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.

25. "Individual" shall mean a natural person or, if appropriate in the context in which it occurs, the Individual's legal representative, authorized to act for the Individual under Applicable Law for matters relating to Data.

26. "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.

27. "Licensed Service" shall mean a SCeHA Service that involves the use of technology that SCHIP licenses from Licensed Technology Providers and makes available to Participant and Other Participants who agree to comply with requirements, whether set forth in the Agreement, applicable to such service. Examples of Licensed Services include, but are not limited to, secure, point-to-point messaging functionality in accordance with the SCeHA direct protocol and image exchange.

28. "Licensed Technology Provider" shall mean a Person that licenses some or all of the technology infrastructure used by SCHIP to provide SCeHA Services.

29. "Master Patient Index" or "MPI" shall mean an electronic database that maintains a unique index (or identifier) for every Individual who has been, or who during the term of the Agreement becomes, registered as a patient at Participant or at any other Participant in the HIE, whether or not the Individual has Opted-Out as specified in the Agreement.

30. "Message" shall mean a vehicle for transmitting Data between Participants through the HIE or External HIE. The transport protocols by which Messages are exchanged include, but are not limited to, Query-Retrieve, Push, and Publish-Subscribe. 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.

31. "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.

32. "Monitor" shall mean the review and examination of a Participant's records (including logs), and/or activities to evaluate the utilization levels, efficiency, and technical capabilities of the HIE and a Participant's compliance with the Agreement. This review can be manual, automated, or a combination of both.

33. "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, or as provided in Section 14 of these Policies and Procedures.

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

35. "Other Participant" shall mean (i) health care providers, (ii) nonhealthcare providers, such as payers and individuals engaged in population health management, care management, or quality improvement, in each case, to the extent permitted by Applicable Law to be a participant in SCeHA, or (iii) community based organizations who provide social service or other supports and who have secured patient authorization to access Electronic Health Information, or (iv) government agencies, in each case, who sign an agreement in substantially the same form as this Agreement or such other form as is deemed appropriate by SCeHA.

36. "Participant" shall mean the person that executes the Participation Agreement, provided that this Agreement may be executed on behalf of multiple related entities by a parent or other entity with

authority to do so, in which case the individual entities shall be listed on Exhibit to this Agreement captioned "Participating Entities" and each facility, provider, or entity so listed shall be individually entitled to the rights and subject to the obligations set forth in this Agreement provided that SCeHA may require Other Participants to separately execute and be bound by another form of Participation Agreement. A "Participant" includes (i) an organization that oversees and conducts, on its own behalf and/or on behalf of its Authorized 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 Authorized Users and has the organizational infrastructure and legal authority to comply with the obligations in this Agreement and to require its Authorized Users to comply with applicable requirements in this Agreement. All Participants must enter into a Participation Agreement with SCHIP or DURSA with the eHealth Exchange and abide the terms and conditions contained therein. References to Participant will also include references to Authorized Users where the context so requires.

37. "Participant Member" means a member of an HIO that is a Participant of SCeHA. A Participant Member must execute a Participation Agreement and pay the requisite 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 SCeHA Policies and Procedures.

38. "Participation Agreement" shall mean the underlying Participation Agreement entered into between each Participant and SCHIP, which outlines the terms of the SCeHA Services.

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

40. "Physician Address Book" or "PAB" shall mean the electronic database of all Authorized Users among whom a Message can be sent and/or from whom a Message can be received, including physicians and other non-physician users of the HIE.

41. "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, SCeHA, contained herein and incorporated into this SCeHA Policy Manual, as they may be amended from time to time.

42. "Policy Manual" means the documents approved by the Governing Authority containing these Policies and Procedures, 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 Policy Manual, as it may be amended. The Governing Authority shall review and may amend the Policy Manual from time to time as provided in the Participation Agreement and in Section 14 of these Policies and Procedures.

43. "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.

44. "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 an 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.

45. "Public Purpose" is a disclosure of Data to public health officials, government agencies, or emergency medical services and others when required by Applicable Law or when permitted by Applicable Law and consistent with the mission of the HIE to advance the health and wellness of South Carolina patients by deploying health information technology solutions adopted through cooperation and collaboration and to enable the South Carolina healthcare community to appropriately and securely share data, facilitate, and integrate care, create efficiencies, and improve outcomes, provided that any disclosure of Data that is permitted, rather than required, by Applicable Law to a recipient other than public health officials, government agencies, or emergency medical services shall not be a Public Purpose unless it is approved by the Board under the process and standards specified in the Agreement.

46. "Publish-Subscribe" shall mean: (i) a patient-specific Message transmitted to a Participant through the HIE indicating the availability of clinical information; (ii) information indicating a patient encounter with a specific Individual has occurred; or (iii) the Push of clinical information that is automatically sent to a Participant who has requested that the HIE automatically provide all available Messages as to a specific Individual.

47. "Push", as to a Message, shall mean clinical information transmitted directly to an Authorized User identified in the Message as a recipient. Push shall apply to all Messages transmitted through the HIE other than Publish-Subscribe or Query-Retrieve, including but not limited to Messages routinely transmitted to ordering or referring physicians, such as reports of imaging or clinical laboratory results.

48. "Query-Retrieve", as to a Message, shall mean a transmission in response to an electronically-generated request by a Participant for transmission of Data of an Individual available through the HIE.

49. "Recipient" shall mean a recipient of Data transmitted through the HIE or SCeHA Services or the recipient of Confidential Information as defined in the Agreement. Recipient, as to the HIE, shall include Authorized Users.

50. “Registry” shall mean the electronic database that maintains metadata about each discrete patient record maintained about an Individual by Participant and all other Participants, including a link to the document in the System in which it is stored. The Registry responds to queries from Participant and other Participants through the HIE about documents meeting specific criteria.

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

52. “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.

53. “SCeHA” means the South Carolina eHealth Alliance, which providesthe secure, standards-compliant technology and policy framework that enables the electronic discovery, query, and retrieval of key clinical Data at the point of care. SCeHA functions such that Participants query and retrieve clinical Data directly from other Participants involved in the provision of a patient’s care using standards-compliant electronic health record systems and SCeHA technology services. Services associated with SCeHA include a statewide Master Patient Index, Record Locator Service, terminology standards and services, trusted uniform transport, Public Key Infrastructure certificate-based encryption and authentication, and audit/log of document transport between Participants.

54. “SCeHA Services” shall mean all services provided by SCeHA for access to and maintenance of Data, including, but not limited to, the availability of the HIE for Permitted Purposes, value-added services (such as care alerts, summaries of care, and status alerts), External HIE Services, and Licensed Services.

55. “SCeHA Website” shall mean www.SCeHA.org. SCeHA may establish a secure section of the Website for Participants for purposes of the Agreement, including but not limited to Notices as provided in the Agreement.

56. “SCHIP” means South Carolina Health Information Partners, Inc., a South Carolina nonprofit corporation, the Governing Authority for SCeHA.

57. “Submitter” shall mean the Participant(s), Participant Member(s), or Authorized User(s) who submit Message Content through a Message to a Recipient for a Permitted Purpose.

58. “System” shall mean SCeHA’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.

59. “Transact” or “Transaction” means to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content using the SCeHA Performance and Service Specifications.

60. “Treatment” shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

# Appendix B – Sample Authorized User Agreement

**AUTHORIZED USER AGREEMENT**

South Carolina Health Information Partners, Inc. ("SCHIP") currently has a Participation Agreement with each data-contributing hospital ("Participants") and with all other provider and payer organizations that access Data. The Participation Agreement includes specific provisions governing the use of Data and includes a Business Associate Agreement. These agreements and SCeHA's Policies and Procedures can be found at www.SCeHA.org. Any capitalized terms in this Authorized User Agreement, unless otherwise defined, have the meaning given to them in the Participation Agreement.

I, the undersigned individual below, as a condition of being granted access to SCeHA Services as an Authorized User, hereby acknowledge, represent, and agree to the following "Terms and Conditions":

1. I acknowledge and understand that SCeHA makes patient information available to only authorized individuals and organizations for treatment, care coordination, quality improvement, and other Permitted Purposes, as identified in the Participation Agreement. I understand that I am a designated Authorized User of Data of on behalf of my sponsoring Participant;

2. By signing below, I agree to comply with all Terms and Conditions of access to Data under this Authorized User Agreement, the Policy Manual, and applicable state and federal laws and regulations;

3. I understand that this is a BINDING agreement, and that my failure to comply with these Terms and Conditions may be grounds for discipline, including without limitation, denial of my privileges to access the SCeHA Services;

4. I understand that I may access patient information only for Permitted Purposes specific to my role and responsibilities in Participant;

5. This Authorized User Agreement grants to me a nonexclusive, nontransferable right to access SCeHA , which is specific to me, and I may not share, sell, or sublicense this right with anyone else, nor change, reverse engineer, disassemble, or otherwise try to learn the source code, structure, or ideas underlying SCeHA's Services, nor connect or install unauthorized or uncertified equipment, hardware, or software, or improperly use the hardware or software relating to use of SCeHA Services;

6. As an Authorized User, I may have access to Data that includes patient information that includes Protected Health Information and is subject to confidentiality, privacy, and security requirements under state, district, and federal law and regulations, and I hereby specifically and expressly agree that I will only access such information consistent with my access privileges, and pursuant to all requirements under these Terms and Conditions;

7. I understand that I have an obligation to maintain the confidentiality, privacy, and security of the Data, and that I will not disclose any Data except as required for the performance of my duties as an employee or agent of Participant and subject to all these Terms and Conditions;

8. At any time after my employment/business relationship with the Participant has ended, I agree to keep confidential any and all information which I obtained as a result of my access to the Data;

9. I will not make any unauthorized copies of Data, and will not save any Data outside of the SCeHA Services;

10. I will not email any Data to another email account, except as expressly provided for in the secure network messaging environment provided by the SCeHA Services or the approved secure and encrypted email solution provide by the Participant;

11. I ACKNOWLEDGE THAT MY AUTHENTICATION CODE AND PASSWORD IS THE LEGAL EQUIVALENT OF MY SIGNATURE, AND THAT I WILL NOT DIVULGE, RELEASE, OR SHARE MY AUTHENTICATION CODE OR DEVICE OR PASSWORD WITH ANY OTHER PERSON, INCLUDING ANY EMPLOYEE OR PERSON ACTING ON MY BEHALF, AND SHALL NOT PERMIT OR AUTHORIZE ANYONE ELSE TO ACCESS SCeHA SERVICES UNDER MY AUTHENTICATION CODE OR DEVICE OR PASSWORD, AND FURTHER AGREE NOT TO USE OR RELEASE ANYONE ELSE'S AUTHENTICATION CODE OR DEVICE OR PASSWORD;

12. I acknowledge that I am responsible for all usage on my accounts, and that my account usage may be monitored at any time;

13. I agree to notify SCHIP and Participant immediately if I become aware or suspect that another person has access to my authentication code or device or password or if I have reason to believe that the confidentiality of my password is broken or believe that there has been a misuse of Data;

14. I agree to log out of the SCeHA Services before leaving my workstation to prevent others from accessing the Data;

15. I agree never to access Data for "curiosity viewing," which includes accessing Data of my family members, friends, or coworkers, celebrities, public figures, etc., unless access is necessary to provide services to a patient related to a direct treatment relationship;

16. I understand that SCeHA uses a privacy tool for additional monitoring of all users' activity around PHI access to ensure all provisioned accounts are being used appropriately and to protect personal health information.

17. I will, to the best of my ability, ensure and protect that Data submitted or received through the SCeHA Services is accurate and agree not to insert or enter any information into the SCeHA Services, including through the Participant's electronic health record, that I know is not accurate;

18. I acknowledge and agree that SCHIP and Participant have the right at all times, including without my consent or notice to me, to monitor, access, review, audit, and disclose my access to and use of the HIE and compliance with the terms of this Authorized User Agreement, the Participation Agreement, the Policies and Procedures, and Applicable Law, including any hardware or software located at my office, home, or any other site from which I access SCeHA Services;

19. By signing below, I acknowledge and agree that I have completed all required training for the SCeHA Services, including on the permissible and prohibited practices relating to the access and use of the SCeHA Services, and agree to abide by all information covered during such training;

20. If I unlawfully access or misappropriate Data, including patient information, I agree to indemnify and hold harmless SCHIP and Participant, their subsidiaries, affiliates, and their successors and assigns against and from any and all claims, demands, actions, suits, proceedings, costs, expenses, damages, and liabilities, including reasonable attorney's fees arising out of, connected with or resulting from such unlawful use;

21. I certify that the documents and information I provide to the SCeHA Services in order to authenticate my identity and demonstrate my professional credentials is current, accurate, and authentic, and I acknowledge and understand that if I present false documents for these purposes, this may subject me to criminal, civil, and other repercussions; and

22. This Authorized User Agreement will be in effect from the time it is signed until SCHIP or Participant terminates my status as an Authorized User or until I violate the Terms and Conditions, and any Terms and Conditions necessary to protect SCHIP, the SCeHA Services and the Data will survive the termination of this Agreement.

By signing below, I have read and agree to abide by all Terms and Conditions of access and use to the SCeHA Services as set forth in this Authorized User Agreement.

Please Print Clearly – ALL FIELDS ARE REQUIRED

**Full Name (First, Middle, Last):**

**Signature:**

**Professional Title:**

**Cell Phone:**

**Primary E-mail:**