



## The South Carolina Health Information Exchange

### Introduction

The South Carolina Health Information Exchange (SCHIEEx) is a statewide technology and policy framework that enables the secure and confidential exchange of electronic patient information according to nationally recognized standards. Participating providers electronically share key clinical information such as medical histories, medications, allergies, diagnoses, and procedures with each other regarding patients they share. Health information exchange is an important tool in improving the quality and efficacy of care a patient receives, reducing duplicative services, enhancing public health and disease detection and monitoring, and improving a patient's health care experience overall.

Participant organizations legally agree to abide by all policies and procedures that govern the operation of SCHIEEx and the privacy and security of health information. The Participant in turn requires each user to sign a User Agreement. This establishes a "chain-of-trust" that is essential for SCHIEEx and each Participant and User to maintain patient trust. Information about SCHIEEx and the SCHIEEx Policy Manual can be found at [www.SCHIEEx.org](http://www.SCHIEEx.org)

### Services

**SCHIEEx DIRECT** is a simple and secure, "point-to-point" clinical messaging service that facilitates communications and information sharing for the delivery and coordination of health care services. Information may be shared for any purpose that is allowed by law. "Point-to-point" means the message is created and sent by one user directly to another known user.

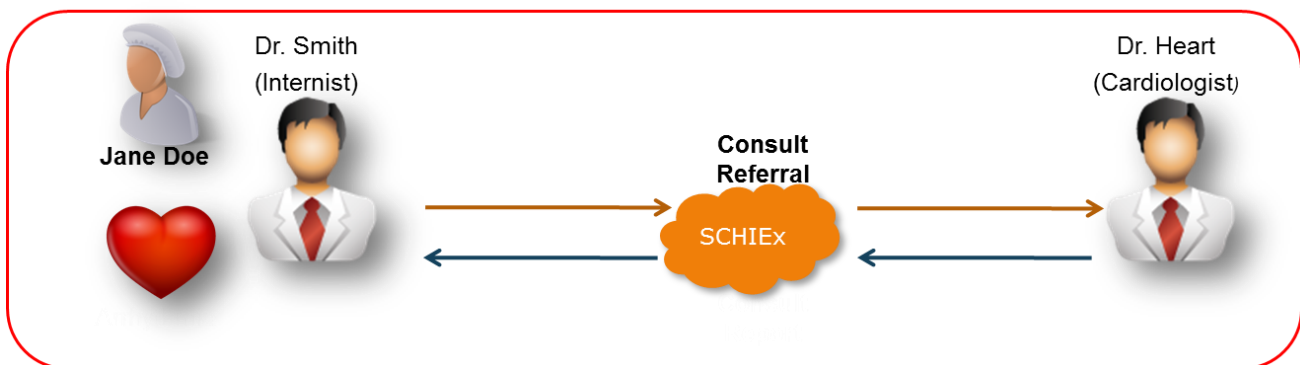
**SCHIEEx EXCHANGE** is a robust, fully automated and bi-directional electronic health information exchange. Participants using Electronic Health Record (EHR) systems and SCHIEEx EXCHANGE technology services "connect" and seamlessly discover and exchange medical summaries regarding shared patients. Information may be shared for treatment and public health and quality reporting purposes. Participants inform patients about SCHIEEx EXCHANGE participation and address questions. Patients can opt out of having information shared via EXCHANGE and Participants must document and execute the patient's wishes.

**SCHIEEx Clinical Viewer** is a secure Web-based application that enables Participants that are not connected to robust EXCHANGE to access needed information available via the Exchange for permitted purposes.



## SCHIEEx DIRECT Key Points

- SCHIEEx DIRECT complies with national specifications for secure directed exchange. Protected Health Information including information subject to special protections may be sent via DIRECT.
- Services include security and trust services, certificate-based encryption and authentication, DIRECT addresses, and message transport and delivery.
- DIRECT messaging can be thought of as a standards-based, secure and encrypted "Health Email". Users send messages, attach documents to messages, and receive messages.
- Each Participant is assigned a unique SCHIEEx address or addresses that are used to direct the message transport from the sender to the intended receiver. Each Participant Site Administrator authorizes individual users, ensures a user agreement is signed, and provides the DIRECT address (or account). The address may be individual level (Dr. I.T. Smith) or entity level (Smith Family Practice or Smith Hospital Emergency Department). The user is provided a SCHIEEx issued user name and password.
- A Participant may use an EHR system, client email system, or the SCHIEEx Web portal as the method to access DIRECT.
- Participants use internal policies/procedures in accordance with applicable state and federal law to designate how the account will be used and appropriately monitored and how access will be controlled and delegated if necessary to authorized users.
- Users should be familiar with Participant security policies and DIRECT security best practices. Participants that utilize the SCHIEEx DIRECT Portal manage security for messages/attachments that are downloaded or saved on local computers. When client email or an EHR is used, the Participant manages security from the point the message is delivered to the Participant's DIRECT address. DIRECT security best practices are located at [www.SCHIEEx.org](http://www.SCHIEEx.org)



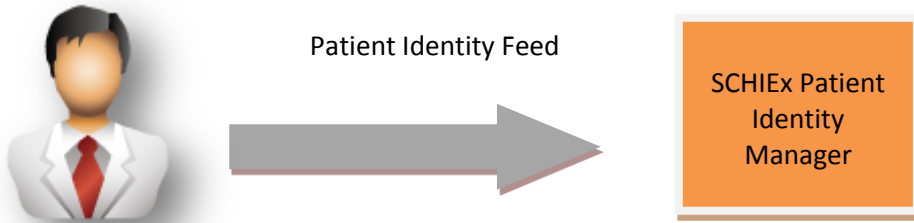


## SCHIEEx EXCHANGE Key Points

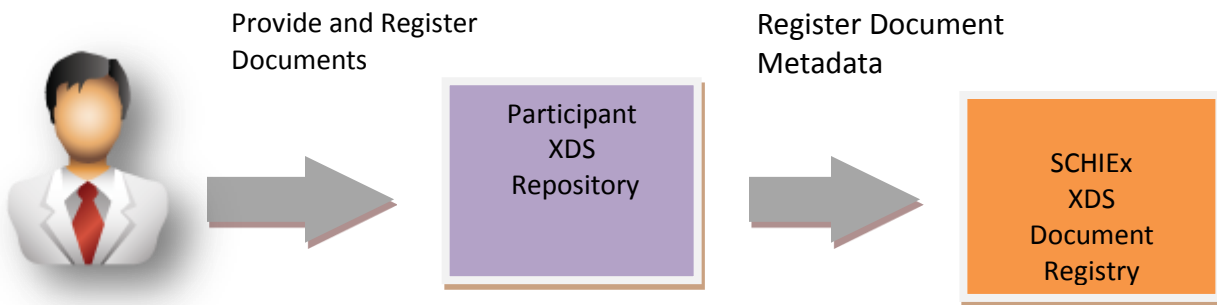
- SCHIEEx EXCHANGE is based on a document sharing model for health information exchange called Integrating the Health Enterprise. Participants share medical summary documents through an EHR system.
- Services include a statewide Master Patient Index, Record Locator Service, terminology standards, trusted uniform transport and certificate-based encryption and authentication, and audit/log of document transport between Participants, and gateways that enable bidirectional exchange with the SCDHEC Immunization Registry and eHealth Exchange (formerly nationwide health information network).
- Because users access available clinical information using their own EHR system, the patient must be registered in the EHR before any information can be retrieved via SCHIEEx.
- The EHR system provides users with an interface to access and view information via SCHIEEx. The steps a user takes to access information via SCHIEEx is different for each EHR system. Each Participant Site Administrator authorizes individual users and ensures a user agreement is signed.
- The EXCHANGE is fully automated and always “on”. Participant EHR systems query and retrieve information when it is needed for patient care.
- Participants using SCHIEEx EXCHANGE must provide patients with written Notice about their participation that includes information about the right to opt out. Opt Out is system-wide or “global”. This means no information can be shared via robust SCHIEEx EXCHANGE or the Clinical Viewer by any Participant regarding a patient that opts out.
- Some EHR systems may offer multiple consent functionalities and options. Participants and users must implement a process that ensures the correct option is utilized to fully execute a SCHIEEx level opt out. SCHIEEx provides a Web-based opt out tool to use when systems do not send this information electronically to SCHIEEx.
- Participants decide what documents and information will be made available to other EXCHANGE Participants. Participants and users must take necessary steps to block information that may be subject to special protections from EXCHANGE. The EHR system provides the functionality and tools so they are different for each system. Participants must implement a process that ensures necessary steps are taken to block information and users are trained accordingly.

# How SCHIEx EXCHANGE Works

## Step 1- Provide Patient Identifiers



## Step 2 - Provision documents for exchange to a cross sharing (XDS) document repository and register document metadata with SCHIEx.



## Step 3- Query and Retrieve





### SCHIEEx Clinical Viewer Key Points

- Services include a secure Web application. Authorized users perform a manual query for documents that are available in SCHIEEx EXCHANGE for a patient with whom the user has established or is in the process of establishing a treatment relationship with and view these documents.
- The Clinical Viewer is always “on” and can be access when needed for patient care.
- Participants using SCHIEEx Clinical Viewer must provide patients with written Notice about their participation that includes information about the right to opt out. Opt Out is system-wide or “global”. This means no information can be shared via robust SCHIEEx EXCHANGE or the Clinical Viewer by any Participant regarding a patient that opts out.
- SCHIEEx provides a Web-based opt out tool to use.