SCHIEx
1919 Blanding Street
Columbia, SC 29201
Phone: 803-898-9962
Fax: 803-898-9972
E-mail: SCHIExInfo@ors.sc.gov
www.SCHIEx.org

Best Practices: Identify a Privacy Officer and a Site Administrator

Reference: SCHIEx Policy Manual, Sections 5b and 11b, respectively

It is the responsibility of the Participant to identify a Privacy Officer and a Site Administrator; these should be two separate positions. In small organizations employing fewer than 10 people, one person may serve as both the Privacy Officer and Site Administrator.

Privacy Officer

Most health care organizations employ a Privacy Officer or Compliance Officer. The Privacy Officer is responsible for keeping the organization up-to-date on federal and state privacy laws and regulations, developing and implementing internal policies and procedures, conducting any internal investigations in the event of a potential breach, and for reporting all breaches in accordance with SCHIEx policy.

SCHIEx policy requires the reporting of any actual or suspected impermissible use or disclosure of protected health information within 48 hours of discovery, regardless of whether the data are encrypted or not encrypted.

Reports of actual or suspected breach must be submitted in writing using the electronic Breach Notification Form that is available at https://SCHIExsub.org, including a contact phone number for the Participant's Privacy Officer. Within 20 hours of reporting the initial breach, the Privacy Officer must submit an update. This allows the SCHIEx staff to submit the required update to the Nationwide Health Information Network within the time frame specified in the DURSA (Data Use and Reciprocal Support Agreement).

Site Administrator

The Site Administrator responsibilities include:

Staff training: A Site Administrator may oversee the development and implementation of the SCHIEx Training or take full responsibility for the development and implementation of the SCHIEx Training program. SCHIEx Training must be documented and documentation must be maintained.

Execute user agreements: Upon completion of SCHIEx Training, the Site Administrator is responsible for having each staff member that is authorized to access SCHIEx sign a User Agreement.

Assign and maintain logins and passwords: Authorization to SCHIEx should only be given to those staff members and contractors who have a legitimate and appropriate need to access SCHIEx, completed SCHIEx training, and executed a User Agreement. The Particpant's electronic medical record should have the ability to authorize users based on the staff member's role within the organization.

> *Example: Doctors will have full access to a patient's medical record; in contrast, a front desk staff member may have access to a patient's demographic information to schedule appointments.*

Logins and passwords should be assigned in accordance with the Participant's internal security policies and procedures.

Monitor access: The Participant's electronic medical records system is likely to come equipped with a mechanism for monitoring who is accessing patient records and when that access happens via a date/time stamp. It is this mechanism that enables the Site Administrator to monitor the use of SCHIEx, maintain an audit log of access, and identify improper access and breaches. Internal policy (and experience) will determine how often a Participant reviews the access logs. Examples of "red flags" may include but are not limited to:

- Repeated queries on similar names
- Several queries in a short period of time
- Queries on famous names, family members, friends
- Someone other than an authorized user accessing the system via a shared log-in/password
- Access during non-work hours

Enforce policies for logins and passwords: Enforcement should follow internal policies and procedures.

Terminate access: In the event an authorized user leaves the Participant organization, voluntarily or otherwise, access to SCHIEx must be terminated in accordance with internal security policies.

SCHIEx Contact

The Participant must identify a contact to receive SCHIEx Policy Manual updates. This individual will receive all official notifications of SCHIEx Policy Manual updates on behalf of the Participant. The contact must have the necessary knowledge and role within the organization to manage internal dissemination of official notifications and to ensure appropriate response on behalf of the Participant. Often the SCHIEx contact is the Participant's Privacy Officer.

Sharing Responsibilities

The responsibilities listed for the Privacy Officer and Site Administrator may be distributed between the two positions differently than listed depending on your organization. For example, the Privacy Officer may assume the training role and execute the User Agreements prior to the Site Administrator assigning the logins and passwords.

The importance of assigning the two positions to two different employees is that the Site Administrator is responsible for assigning logins and passwords. If that information gets into the wrong hands, even inadvertently, the Site Administrator cannot investigate him or herself. For liability purposes, the Privacy Officer or other staff member should be conducting the internal investigation. For small practices that are part of a Regional Health Information Organization or other Health Information Organization, a third-party can assume the role of Site Administrator.