TITLE: CONNECTDIRECT OPERATIONAL SECURITY POLICY	
STATUS: FINAL	**EFFECTIVE DATE: 03/01/2022**
VERSION: 3	**PAGE: 1 OF 2**

I. PURPOSE

This Policy defines the security requirements for Participants and Participant Users of the ConnectDirect Service. It is the policy of CCHIE to ensure that user accounts and systems are properly authenticated and controlled to ensure that only appropriate access to information occurs.

II. SCOPE

This Policy applies to CCHIE and Participants and Participant Users of CCHIE's ConnectDirect Service.

III. POLICY

A. Each Participant must designate a resource to act as its ConnectDirect Administrator.

B. Participant Administrators shall require identity verification.

C. Participant and/or Participant Administrator shall verify the identity and appropriateness of its Participant Users.

D. Participant User account requests shall be approved by the Participant and/or Participant Administrator.

E. Participant and Participant Users shall ensure passwords are unique and confidential.

F. Participant and Participant Users shall take security precautions in the workspace such as the use of password screen locks, session timeouts, and logging out of workstations at the end of the working day.

G. Participant and Participant Users shall take reasonable precautions to secure their physical working environment against unauthorized access.

H. ClinicalConnect HIE provides production and maintenance support to Participants. Note that Participants provide the first line of Participant User support to their

Authorized Personnel and may escalate issues and questions to the ClinicalConnect HIE support account.

I. If Participant and Participant Users suspect that an account has been compromised, the account owner shall change his or her password immediately and contact the appropriate Participant Help Desk/Support Entity to investigate a potential security breach. If a breach is suspected of any system, administrative, or user account, all potentially compromised account passwords shall be immediately changed and the appropriate Help Desk/Support Entity, including the CCHIE support account, shall be notified to initiate an investigation into the potential security breach.

J. Participants are responsible for auditing all accounts within the Administrator's oversight, including those associated with group Direct Email Accounts to ensure appropriate use of the ConnectDirect Service and will take appropriate action to discipline for inappropriate use of CCHIE's ConnectDirect Service or use/access of heath data.

K. CCHIE will provide transaction log reports upon request to support Participants' Accounting of Disclosure requests, auditing, and breach investigations.

L. CCHIE may publicly disclose a list of Participants through its website and/or marketing materials. CCHIE may publicly disclose overall ConnectDirect transaction volume and transaction volume by Participant type (e.g., Provider, Payer, Public Health Agency). CCHIE will not publicly disclose transaction volume by Participant, unless approved by the Participant, or as required by law.

IV. Revision History

DATE	AUTHOR	COMMENTS
3/2018 – 8/2018	Dianne Clark, Laura Mosesso and Joanne Onyshko	Initial draft of CCHIE HISP Service Policies
2/16/2022	Laura Mosesso	Updated HISP Services to ConnectDirect Service, updated verbiage for applicability and consistency across all ConnectDirect materials.
3/1/2022	Laura Mosesso	Finalized Policy