ClinicalConnect
Health Information Exchange

TITLE: INFORMATION SYSTEMS SECURITY OVERSIGHT	
STATUS: FINAL	**EFFECTIVE DATE: October 1, 2019**
VERSION: 7	**PAGE: 1 OF 2**

I. PURPOSE

ClinicalConnect HIE's (CCHIE) Security and Compliance Analyst is accountable for electronic information security, related policies, and the execution and use of security measures necessary to protect CCHIE's electronic information.

II. OVERVIEW

This policy defines the duties and responsibilities of the security official, which include the development and implementation of CCHIE's information security policies and procedures.

III. SCOPE

This policy applies to CCHIE employees, contractors, and Participants.

IV. POLICY

A. CCHIE's President authorized that the guidance, direction, and authority of CCHIE information security activities shall be centralized under the oversight of CCHIE's Security and Compliance Analyst. Information security activities include computer system user account management and information security functions

B. CCHIE shall maintain a security plan for all systems and applications under the area of responsibility, in accordance with the system security plan standards maintained by the UPMC Information Assurance Services.

C. Users of CCHIE Systems are responsible for adherence to all relevant policies standards, procedures, and regulatory requirements.

D. If an exception to any security policy or standard is required, the CCHIE Security & Compliance Analyst or other Compliance Team member must be timely notified so that the exception can be appropriately documented and, if necessary, submitted for approval.

E. CCHIE's Security and Compliance Analyst has oversight for:

1. Documenting/implementing information security policies, standards and procedures;

2. Creating and maintaining information security awareness training for all CCHIE employees and contractors all workforce members;

3. Monitoring compliance with information security policies, processes, standards, and procedures and referring problems to the appropriate department staff or system administrators;

4. Monitoring internal control systems that ensure appropriate user access levels and security clearance to information systems is compliant with the minimum necessary and least privilege principle, as well as ensuring applications are securely maintained;

5. Performing information security risk assessments and reviews;

6. Monitoring advancements in information security technologies; and

7. Monitoring changes in legislation and accreditation standards that affect information security.

IV. Revision History

DATE	AUTHOR	COMMENTS
09/09/2015	Erika Jones	Creation of policy
09/13/2016	Jones/Szymanski	Reviewed policy – no changes
07/23/2019	Keith Dukes	Modified the purpose, updated section E, removed/modified responsibilities, and updated format to the new template
06/29/2020	Keith Dukes	Reviewed – Minor Changes
08/14/2020	Keith Dukes	Reviewed – Minor Changes
07/21/2021	Keith Dukes	Reviewed – No Changes
08/24/2022	Keith Dukes	1. In section B, changed “Information Security Group” to “Information Assurance Services”. 2. In section D, updated language to submit security exceptions to the CCHIE Security & Compliance Analyst or CCHIE Compliance Team for documentation and approval. 3. Adjusted grammatical error in section E list. 4. Updated spacing throughout policy.