ClinicalConnect
Health Information Exchange

TITLE: INFORMATION SYSTEMS SECURITY OVERSIGHT	
STATUS: FINAL	**EFFECTIVE DATE: October 1, 2019**
VERSION: 4	**PAGE: 1 OF 2**

I. PURPOSE

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

II. OVERVIEW

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

III. SCOPE

This policy applies to ClinicalConnect HIE employees, contractors, and Participants.

IV. POLICY

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

B. ClinicalConnect HIE 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 ISD Information Security Group

C. Users of ClinicalConnect HIE information 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, it must be documented appropriately within the system security plan Risk Awareness to Owner (RATO) notification or documented within the appropriate exception process managed by UPMC's security team.

E. ClinicalConnect HIE'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

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

IV. Revision History

DATE	AUTHOR	COMMENTS
9/9/2015	Erika Jones	Creation of policy
9/13/2016	Jones/Szymanski	Reviewed policy – no changes
7/23/2019	Keith Dukes	Modified the purpose, updated section E, removed/modified responsibilities and updated format to the new template
6/29/2020	Keith Dukes	Reviewed – Minor Changes