

TITLE: INFORMATION SYSTEMS SECURITY OVERSIGHT	
STATUS: FINAL	EFFECTIVE DATE: 09/09/2015
VERSION: 1	PAGE: 1 OF 2

I. PURPOSE

Information security shall be secured to appropriately protect the confidentiality and integrity of all patient, personnel, business, academic, and research information, and ensure that such information is made available on a need-to-know basis.

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 staff, 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 the UPMC ISD Information Security Group.

- E. ClinicalConnect HIE’s Security and Compliance Analyst has oversight for:
 1. Establishing ClinicalConnect HIE’s information security architecture
 2. Documenting/implementing information security policies, standards and procedures
 3. Creating and maintaining information security awareness training materials for all workforce members to take
 4. Monitoring compliance with information security policies, standards, and procedures and referring problems to the appropriate department staff or system administrators
 5. Monitoring internal control systems that ensure appropriate user access levels and security clearance to information systems and ensuring applications are securely maintained
 6. Performing information security risk assessments and reviews
 7. Monitoring advancements in information security technologies
 8. Monitoring changes in legislation and accreditation standards that affect information security.
 9. Initiating, facilitating, and promoting activities to foster information security awareness within the organization serving as the information security liaison for users of clinical, administrative, and business systems

V. Revision History

DATE	AUTHOR	COMMENTS
9/9/15	Erika Jones	Creation of policy
9/13/16	Jones/Szymanski	Reviewed policy – no changes