Risk Management Program for the Advanced Computational Health Enclave

Document Name: Advanced Computational Health Enclave Risk Management Program
Version: 2.0
Accountable: James Eyrich
Authors: Alex Withers

Reviewed: Nov 6, 2023
Approved: Dec 20, 2019

Purpose

Risk Management Program to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its sensitive data, including electronic protected health information (ePHI) and controlled unclassified information (CUI). This program enables NCSA to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the NCSA's compliance with the University of Illinois HIPAA Directive and other regulations involving sensitive data. Information produced during the risk assessment will be used to determine and manage security controls for our sensitive data resources.

Scope

This risk management program applies to resources with sensitive data that are managed by the NCSA, including those in the Advanced Computational Health Enclave.

Standards

The risk management program consists of two processes:

1. **Risk Assessment** - Identifies and prioritizes the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place.
2. **Risk Mitigation** - a process that prioritizes, evaluates and implements security controls that will reduce or offset the risks determining the risk assessment process to satisfactory levels within an organization given its mission and available resources.

Risk Assessment Frequency

A risk assessment will be performed every year with coordination of the NCSA Security Office and the NCSA CISO (NOTE: **the NCSA CISO is assumed to also be the NCSA HIPAA Liaison**). Exceptions to this include (i) substantial infrastructure/environment changes that would require a new impact analysis and (ii) a security incident that warrants reevaluation of risks.

Risk Assessment Components

A risk assessment is conducted as per the documented NCSA Risk Assessment and Mitigation procedure. Risks will be recorded in the NCSA risks register, and risk assessments will be saved for 6 years or from the inception of the NCSA Health Care Component.

NCSA implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the confidentiality, integrity, and availability of all sensitive data the organization creates, receives, maintains, and/or transmits,
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of sensitive data,
3. Protect against any reasonably anticipated uses or disclosures of sensitive data that are not permitted or required, and
4. Ensure compliance by workforce members.

Risk Management Process

The risk assessment is part of an ongoing process to understand and manage risk. The broader process contains the following steps as per the documented NCSA Risk Assessment and Mitigation procedure:

- A risk assessment is performed.
- Findings are submitted to the NCSA Security Office within 30 days, and the Security Office forwards them to the CISO.
- The NCSA Security Office works with the project(s) to remediate vulnerabilities and mitigate risks within 90 days of finishing the assessment. If this is not possible for all risks, an exemption must be requested in writing to the Security Office and CISO.
- Remediation activities are documented in a remediation plan.
- The remediation plan is sent to the Security Office, which sends it to the CISO.

Privacy

All data from the risk assessment is kept confidential and not shared without written approval from the NCSA Security Office and CISO.

Consequences

All workforce members are expected to fully cooperate with all persons charged with doing risk management work. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation according to University of Illinois policy, including the University of Illinois HIPAA Directive Sanction policy.