Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements

OPTN Network Operations Oversight Committee

Purpose of Proposal

- Background
  - Increase in recent healthcare malware and ransomware attacks
  - Security frameworks vary by members
  - Individuals are currently bound by the System Terms of Use, but member organizations are not
  - OPTN Contract requirements
- Strengthen the protection of candidate, recipient, and donor data by:
  - Reducing risk of member security incidents
  - Establishing expectations for member response in the event of a security incident that could compromise the security of the OPTN Computer System or its data

Proposal

- The proposal establishes the following:
  - Required security training
  - New appointment of Information Security Contact
  - Member security framework and controls
  - Security readiness assessment, attestation and audit requirements for compliance monitoring
  - Security requests for information regarding potential risks to the OPTN Computer System
  - Incident management response requirements, which could include removal of access to the OPTN Computer System until the risk is mitigated
- The proposal also includes a transition period for member security framework compliance

Potential Phased Approach for Implementation

Prep Work (Spring 2023)

- Users complete Member Security Training and Associated Exam*
- Identify future Information Security Point of Contact*
- Ensure two Site Security Administrators per program*

Transition (Summer/Fall 2023)

- Include notification to the OPTN in your incident response plan*
- Readiness assessment
- Work with OPTN Contractor on Plan of Action to increase security maturity*

Ongoing (2024-2026)

- Members attest annually to meeting the controls of security framework
- Members audited once every three years

*Will become ongoing requirements

What do you think?

- Who in your institution should be engaged as a part of this proposal?
- Is the proposed phased implementation feasible for members?
- What plans does your institution have to maintain operations in the case of a breach?
  - How does transplant fit into this plan?