OPTN

Notice of OPTN Policy Changes

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

Sponsoring Committee:	**Network Operations Oversight**
Policies Affected:	***1.2: Definitions***
	3.1: Access to the OPTN Computer Systems
	3.1.A: Security Requirements for Systems Accessing the OPTN Computer System
	3.1.B: Site Security Administrators
	3.1.C: Security Incident Management and Reporting
	3.1.C.i: Information Security Contact
Public Comment:	**January 19, 2023—March 18, 2023**
Board Approved:	**June 26, 2023**
Effective Date:	**Pending implementation and notice to OPTN members**

Purpose of Policy Changes

These changes enhance the security of the OPTN Computer System by reducing the risk of member security incidents and requiring members to notify the OPTN of security incidents and their resolution. These changes will increase accountability for securing the OPTN Computer System by creating OPTN member-level accountability for individual users' access. Increasing the security of the OPTN Computer System protects candidate, recipient, and donor data, and increases public trust. Furthermore, these additions are necessary to address modifications made to the OPTN Contract as required by Health Resources and Services Administration (HRSA).[1]

Proposal History

The Network Operations and Oversight Committee began developing this proposal in August 2022 in response to security incidents at member institutions. The OPTN Contract was modified later in August 2022 to require the OPTN Contractor to work with the Network Operations Oversight Committee to

[1] By contract with the Department of Health and Human Services, the OPTN Computer System is a contractor-owned, contractor-operated system. The OPTN Contractor owns the computer system that is used as the OPTN Computer System. Requirements for the performance and maintenance of the OPTN Computer System are embedded in the OPTN contract (HHSH250201900001C). HHS recently modified the OPTN contract to require the OPTN Contractor to undertake additional security measures for the OPTN Computer System, including working with the NOOC to establish policy requirements for those members interacting with the OPTN Computer System.

establish policy requirements for members interacting with the OPTN Computer System. This proposal was submitted for Public Comment in January 2023, and to the OPTN Board of Directors in June 2023. Community feedback agreed with the importance of increasing the security of patient data and provided multiple improvement suggestions for the Committee.

Summary of Changes

The proposal establishes the following:

- Security framework and controls for all members with access to the OPTN Computer System, based on the most recent revision of a National Institute of Standards in Technology (NIST) information security framework or a security framework with equivalent controls
- Annual self-attestation from members on the security framework in place
- Auditing every three years and compliance monitoring for security requirements
- Security requests for information
- Development of an incident response plan with the potential for required actions based on the type and scope of the security incident
- Establishment of an information security contact role
- Security training for all member organization staff
- Appointment of at least one additional site security administrator, for a total of two, at minimum per program

Implementation

Summer 2023

Members may begin reporting information security contacts to the OPTN and a second site security administrator immediately. The personnel for these positions must be reported to the OPTN by July 31, 2023, to prepare for implementation of requirements related to security incidents on August 1, 2023. Members will initially report information security contacts via a web form distributed in a communication to members, and later updates will occur via Member Community. Members will report site security administrators via the existing Site Administrator Registration Form.

Members can report security incidents via the OPTN Contractor's Organ Center telephone line at (800) 292-9537. This reporting will be required as of August 1, 2023. The scope of security incidents is limited to declared events involving servers, networks, and devices used to access or manage access to the OPTN Computer System.

Members will also be required to respond to requests for information starting August 1, 2023. Requests for information will be distributed to the members' information security contacts when a known exploited vulnerability that has the potential to affect the OPTN Computer System occurs. These requests for information inform the OPTN Contractor of the state and remediation status of the vulnerability within the member's computing environment.

No Earlier than October 2023

The initial attestation will be a readiness assessment, intended to assess the current state of members' information security framework. The security controls from the National Institute of Standards and Technology (NIST) security framework are not required to be fully implemented at this time. Readiness assessments will begin no earlier than the fourth quarter of 2023, and the OPTN will provide a minimum

30-day notice prior to sending the readiness assessments and provide members with at least three months to complete their assessments. Attestations will be distributed to the members' information security contacts for completion.

No Earlier than June 2024

Audits will begin no earlier than the third quarter of 2024, and the OPTN will provide a minimum 30-day notice prior to beginning audits. Members will receive individual notice via their information security contacts for the timing of their specific audits, and routine audits will occur over a three-year cycle.

Upon Implementation and Notice to Members

All member users who access the OPTN Computer System will also be required to complete information security training specific to the OPTN Computer System on an annual basis. This training will be available within the OPTN Contractor's Learning Management System, and members and users will receive notice after this training is implemented and available. This training will be required annually, and users will be notified at least one month prior to when the training must be completed.

Affected Policy Language

New language is underlined (example) and language that is deleted is struck through (~~example~~).

1.2 Definitions

The definitions that follow are used to define terms specific to the OPTN Policies.

OPTN Computer System

The software platform operated by the OPTN Contractor in performance of the OPTN Contract. This platform includes, but is not limited to, the OPTN Data System, the OPTN Waiting List, the OPTN Donor Data and Matching System, the OPTN Organ Labeling, Packaging, and Tracking system, the OPTN Patient Safety Reporting Portal, and OPTN Kidney Paired Donation Pilot Program (KPDPP).

Security incident

An event that is declared as jeopardizing the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

3.1 Access to the OPTN Computer System~~s~~

~~Only the following categories of members may access the match system:~~

1. ~~Transplant hospitals~~
2. ~~Organ procurement organizations (OPO)~~
3. ~~Histocompatibility laboratories~~

~~The waiting list may only be accessed by members, and members may not use the match system for non-members or add candidates to the waiting list on behalf of non-member transplant hospitals.~~

Transplant hospital, organ procurement organization, and histocompatibility laboratory members are provided access to the OPTN Computer System as members of the OPTN. Transplant hospital, organ procurement organization, and histocompatibility laboratory members with access to the OPTN Computer System may authorize user access to the OPTN Computer System.

Representatives of HRSA, HHS, and other components of the federal government are provided access to the OPTN Computer System as requested by the HRSA COR.

Members must ensure that all users meet OPTN training requirements prior to establishing a user's access to the OPTN computer system and yearly thereafter. Members must also ensure that all users comply with the OPTN Contractor's system terms of use for the OPTN Computer System.

3.1.A Security Requirements for Systems Accessing the OPTN Computer System

Transplant hospital, organ procurement organization, and histocompatibility laboratory members must provide security for the computing environments and components thereof which are used access the OPTN Computer System and the associated environments used to manage the member's computing environment used to access the OPTN Computer System.

Transplant hospital, organ procurement organization, and histocompatibility laboratory members must ensure that these environments adhere to a security framework that is either:

- the most recent revision of a National Institute of Standards in Technology (NIST) information security framework or
- a security framework with equivalent controls provided by the member and approved by the OPTN.

Transplant hospital, organ procurement organization, and histocompatibility laboratory members who authorize access to users must ensure that the user agrees to access the OPTN Computer System through computing environments that adhere to either the most recent revision of a NIST information security framework or a security framework with equivalent controls.

Transplant hospital, organ procurement organization, and histocompatibility laboratory members must attest to their adherence to their security framework through an OPTN attestation. OPTN attestations must be submitted annually and upon request by the OPTN to maintain access to the OPTN Computer System.

Adherence to the security framework will be audited at least once every three years. Transplant hospital, organ procurement organization, and histocompatibility laboratory members must also respond to OPTN requests for information within the timeframe stated by the OPTN.

3.1.B Site Security Administrators

Organ procurement organization and histocompatibility laboratory members with access to the OPTN Computer System must designate at least two site security administrators to maintain access to the OPTN Computer System. Transplant hospital members with access to the OPTN Computer System must designate at least two site security administrators for each of its designated transplant programs.

Site security administrators are responsible for maintaining an accurate and current list of users and permissions, specific to the role of the user in its performance of duties related to OPTN Obligations. Permission levels must be granted according to the NIST principle of least privilege.

Site security administrators must review user accounts and permission levels:

- When a user is no longer associated with the member organization
- When the user's roles or responsibilities have changed, such that a different level of permission is necessitated
- As directed by the OPTN

3.1.C Security Incident Management and Reporting

Transplant hospital, organ procurement organization, and histocompatibility laboratory members with access to the OPTN Computer System must develop and comply with an incident response plan designed to identify, prioritize, contain and eradicate security incidents. The incident response plan must include *all* of the following:

- Appointment of an information security contact, as detailed in OPTN *Policy 3.1.C.i: Information Security Contact*
- Notification to the OPTN Contractor of security incidents occurring in any environment outlined in *Policy 3.1.A: Security Requirements for Systems Accessing the OPTN Computer System*, as soon as possible, but no later than:
    - 24 hours following the information security contact becoming aware of the security incident if a member does not disconnect the affected users and any impacted systems from the OPTN Computer System
    - 72 hours following the information security contact becoming aware of the security incident if the member does disconnect the affected users and any impacted systems from the OPTN Computer System
- Process for acquiring third party validation of proper containment, eradication, and successful recovery

Portions of the incident response plan involving access to the OPTN Computer System must be made available to the OPTN on request and will be considered confidential.

In the event of a security incident, members will be required to provide status updates to the OPTN on the security incident on an agreed upon schedule and to meet control and verification requirements as provided by the OPTN based on the type of security incident. These requirements will be communicated directly to the member through the information security contact established in the member's incident response plan. Members may also be required to provide a final incident report.

Members may be required to take specific actions to appropriately ensure risk to the OPTN Computer System is managed and balanced with the need to ensure transplants continue. Specific actions may include on-site remediation, requiring the member's access to the OPTN Computer System be temporarily removed until the OPTN has determined the risk is mitigated, or other containment and recovery actions with oversight by the OPTN.

Any action that temporarily removes the member's access to the OPTN Computer System must be directed by the OPTN or the Secretary of HHS. The OPTN Contractor may take other actions necessary to secure the OPTN Computer System on behalf of the OPTN. Any actions taken by the OPTN Contractor to secure the OPTN Computer System on behalf of the OPTN must be reported to the OPTN within 48 hours.

3.1.C.i Information Security Contact

Transplant hospital, organ procurement organization, and histocompatibility laboratory members with access to the OPTN Computer System must identify an information security contact, who is responsible for maintaining and complying with a written protocol that includes how an information security contact will:

1. Provide 24/7 capability for incident response and communications
a. Receive relevant notifications of security incidents from the member's information security staff
b. Communicate information regarding security incidents to the OPTN
c. Facilitate development and fulfillment of OPTN Obligations outlined in OPTN *Policy 3.1.A: Security Requirements for Systems Accessing the OPTN Computer System*