Notice of OPTN Policy and OPTN Management and Membership Policy Changes

Revise Conditions for Access to the OPTN Computer System

Sponsoring Committee:	**Network Operations Oversight Committee**
OPTN Policies Affected:	***1.2: Definitions*** ***3.1: Access to OPTN Computer System*** ***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*** ***3.1.D: Non-Member Access***
OPTN Management and Membership Policies[1] Affected:	***F.7: Business Members*** ***Appendix M: Definitions***
Public Comment:	**July 31-September 24, 2024**
Board Approved:	**December 2-3, 2024**
Effective Date:	**Pending implementation and notice to OPTN members**

Purpose of Policy and Bylaw Changes

This proposal aims to enhance the security of the OPTN Computer System by revising conditions for access. This proposal will expand accountability for securing the OPTN Computer System to business organizations who access the OPTN Computer System, many of whom are third party contractors of OPTN members. Enhancing the security of the OPTN Computer System protects candidate, recipient, and donor data, and increases public trust. Furthermore, instituting OPTN interconnection security agreements (ISAs) is necessary to adhere to NIST requirements.[2]

Proposal History

The OPTN Contract requires the OPTN Contractor to work with the Network Operations Oversight Committee to establish policy requirements for members interacting with the OPTN Computer System.

[1] This proposal was originally drafted using the former structure of the OPTN Policies and OPTN Bylaws. On December 2, 2024, the OPTN adopted a new structure of governance, splitting the OPTN Bylaws into two documents: the OPTN Bylaws and OPTN Management and Membership Policies. The references to the affected provisions have been updated to match the format adopted in December. For more information, please see the OPTN proposal *Revised Bylaws and Management and Membership Policies,* available at https://optn.transplant.hrsa.gov/media/vwuovfyu/excom_revised-bylaws-and-management-and-membership-policies_bp.pdf.

[2] National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5. (December 2020).

In June 2023, the OPTN Board approved a proposal to *Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements* which applied to transplant hospital, OPO, and histocompatibility lab members. This proposal was developed to expand these requirements for business organizations accessing the OPTN Computer System. This proposal was submitted for Public Comment in July 2024, and to the OPTN Board of Directors in December 2024. Community feedback agreed with the importance of increasing the security of patient data and provided multiple improvement suggestions for the Committee. Based on these suggestions, the Committee adjusted some areas of the policy language submitted to the Board for approval. In December, the Board approved an amendment to adjust the ISA completion requirement from six months to three months.

Summary of Changes

This proposal changes the following:

- Require OPTN membership as a condition of access to the OPTN Computer System
- Reduce potential barriers to OPTN business membership
- Limit reasons for access to the OPTN Computer System to facilitating organ transplantation, fulfilling OPTN Obligations, and quality assurance and performance improvement (QAPI)
- Require reporting of privacy incidents involving data obtained from the OPTN Computer System
- Require all members with system interconnections to the OPTN Computer System to submit an ISA to the OPTN
- Require OPTN business members who access the OPTN Computer System to follow the same information security requirements that apply to other member types who access the OPTN Computer System

Implementation

This proposal will impact all members with access to the OPTN Computer System. All members will now be required to report privacy incidents of data obtained from the OPTN Computer System. There will be additional impact for members with interconnections with the OPTN Computer System, as well as business organizations. If a member's computer systems connect to the OPTN Computer System, they will be required to complete an ISA within three months of OPTN request, every three years, and update it as connected systems, security, and interconnections change. All members will also need to educate their users on permissible reasons for access to the OPTN Computer System according to proposed policy requirements.

Business organizations who access the OPTN Computer System will need to apply for business membership to the OPTN if they are not already members. All current business members will need to submit the name of an alternate representative and an information security contact. Business members accessing the OPTN Computer System must provide a list of all active OPTN members they are contracted with, update this list and report to the OPTN within seven days of any changes, and verify the accuracy of this list upon request by the OPTN. Business members must also provide copies of their DUAs with each OPTN member they are contracted with to the OPTN upon request. Business members will also need to educate their users on permissible reasons for access to the OPTN Computer System according to proposed policy requirements.

Business members will need to develop a security framework that meets or exceeds controls in NIST SP 800-171, if they do not have such a framework already. This may take significant time and new personnel, depending on the organization's current information security status. Depending on the state of the organization’s information security revealed in the initial attestation, members may be asked to detail compliance and the level of risk through a Plan of Actions and Milestones (POAM) or Risk Based Decision (RBD) with the OPTN Contractor’s information security staff. This would require regular updates to the OPTN Contractor, and remediation in the agreed upon timeframe.

Business members will be required to complete attestations annually, and audits at a minimum of every three years. Required requests for information will be dependent on the cybersecurity landscape, as it is not possible to predict the number of critical and high known exploited vulnerabilities that will be discovered.

Management of a security incident will now need to involve OPTN notification and updates. Members may be required to utilize third-party incident response teams to assist with incident containment and recovery, dependent on the circumstances and severity, as well as to verify to the OPTN that recovery was performed in such a way that access can be securely re-established to the OPTN Computer System.

For the OPTN, the transition plan for this proposal includes review and approval work for business member applications. The ongoing work for this proposal will require additional information security personnel to review business member attestations and perform business member audits every three years. It will require additional information security and information technology personnel to review ISAs of OPTN members who utilize APIs for the OPTN Computer System every three years, and with any interim updates needed.

Affected Policy Language

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

1.2: Definitions

Privacy Incident

A suspected or confirmed incident involving the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information (PII) or (2) an authorized user accesses PII for an other than authorized purpose.

Quality Assurance and Performance Improvement (QAPI)

Any quality assessment and improvement activities consistent with the definition of health care operations in the Health Insurance Portability and Accountability Act (HIPAA).

3.1: Access to OPTN Computer System

Transplant hospital, organ procurement organization, and histocompatibility laboratory members are provided access to the OPTN Computer System as members of the OPTN for the purposes of facilitating organ transplants, quality assurance and performance improvement (QAPI), and fulfilling OPTN Obligations, as defined in *OPTN Management and Membership Policy Appendix M: Definitions*.[3] Business members may be granted access to the OPTN Computer System for the purposes of facilitating organ

[3] Originally located in *OPTN Bylaw Appendix M: Definitions.*

transplants and fulfilling OPTN Obligations, as defined in *OPTN Management and Membership Policy Appendix M: Definitions*, on behalf of affiliated transplant hospitals, OPOs, or histocompatibility labs.

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 also ensure that all users comply with the OPTN Contractor's system terms of use for the OPTN Computer System.

3.1.~~D~~A: ~~Non-Member Access~~ Conditions for Access to and Interconnection with the OPTN Computer System

Members must have an active OPTN Interconnection Security Agreement (ISA) in order to interconnect with the OPTN Computer System, including interconnection via Application Programming Interface (API). The ISA must be executed by an individual authorized by the member organization within three months of being issued by the OPTN, reviewed annually, and renewed every three years.

The member must execute a new ISA with the OPTN:

- Upon change in any of the information provided by the member
- If additional interconnections are required
- If any of the requirements for interconnections change
- At the request of the OPTN

Members may not use the ~~match system~~ OPTN Computer System for non-members or allow non-members access to the ~~match system~~ OPTN Computer System.~~ unless *all* of the following requirements are met:~~

Transplant hospitals, OPOs, and histocompatibility labs may grant business members permissions to their patient-identified data in the OPTN Computer System if *all* of the following requirements are met:

1. The business ~~non-~~member is assisting the member with facilitating organ transplants~~, placing organs for purposes other than transplantation, or reporting data to the OPTN.~~ or otherwise fulfilling OPTN Obligations, as defined in *OPTN Management and Membership Policy Appendix M: Definitions.*[4]
2. The business member users are granted access to the OPTN Computer System according to *OPTN Policy 3.1.C.i: Business Member Users within the OPTN Computer System.*
3. The ~~member~~ transplant hospital, OPO, or histocompatibility lab has a ~~data use agreement (~~DUA~~)~~ with the business ~~non-~~member with *all* of the following elements:
   a. Data confidentiality and security requirements
   b. Data rights
   c. Access to patient-identified data

[4] Originally located in *OPTN Bylaw Appendix M: Definitions.*

d. Data use
e. Procedures for securing data confidentiality
f. Storage or disposal of data upon completion of contracted task
g. Procedures to protect patient-identified data in the event of a data breach, inadvertent or otherwise
h. Remedies in the event of a violation of the DUA

The member must maintain copies of all DUAs with business ~~non-~~members.

Business members accessing the OPTN Computer System must provide a list of all active OPTN members they are contracted with, update this list and report to the OPTN within 7 days of any changes, and verify the accuracy of this list upon request by the OPTN. Business members must also provide copies of their DUAs with each OPTN member they are contracted with to the OPTN upon request.

If the business member is no longer contracted with any active OPTN members they must notify the OPTN within 7 days prior to the contract ending and their access to the OPTN Computer System will be removed upon contract end.

Transplant hospitals, OPOs, and histocompatibility labs must notify the OPTN within 7 days prior to the contract ending when they are no longer contracted with a business member.

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

~~Transplant hospital, organ procurement organization, and histocompatibility laboratory~~ M~~m~~embers must provide security for the computing environments and components thereof which are used to 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~~ M~~m~~embers must ensure that these environments adhere to a security framework that is either:

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

~~Transplant hospital, organ procurement organization, and histocompatibility laboratory~~ M~~m~~embers 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~~ M~~m~~embers 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~~ M~~m~~embers must also respond to OPTN requests for information within the timeframe stated by the OPTN.

3.1.~~B~~C: Site ~~Security~~ Access Administrators

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

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

Site ~~security~~ access administrators must review and update user accounts and permission levels:

- When a user is no longer associated with the member organization, as soon as possible, but no later than 24 hours after the user’s last day of employment
- When the user’s roles or responsibilities have changed, such that a different level of permission is necessitated, as soon as possible, but no later than 24 hours from the change in roles or responsibilities
- As directed by the OPTN, within the timeframe provided by the OPTN

3.1.C.i: Business Member Users within the OPTN Computer System

Business member representatives are responsible for maintaining an accurate and current list of users. The list must include all organizations for which the user requires OPTN Computer System access. Business member representatives must review user accounts:

- When a user is no longer associated with the business member
- When a user's affiliated organizations have changed
- As directed by the OPTN

Business member representatives must report changes in user accounts to the OPTN:

- When a user is no longer associated with the business member, as soon as possible, but no later than 24 hours after the user’s last day of employment
- As directed by the OPTN, within the timeframe provided by the OPTN

Business member users are granted access to the OPTN Computer System by the OPTN Contractor. Business member users are granted permissions to data within the OPTN Computer System by the site access administrators at each affiliated organization according to the NIST principle of least privilege.

3.1.~~C~~D: Security Incident and Privacy Incident Management and Reporting

~~Transplant hospital, organ procurement organization, and histocompatibility laboratory~~ M~~m~~embers 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 and privacy incidents. The incident response plan must include *all* of the following:

1. Appointment of an information security contact, as detailed in *OPTN Policy 3.1.~~C~~D.i: Information Security Contact*
    - Notification to the OPTN Contractor of security incidents occurring in any environment outlined in *OPTN Policy 3.1.~~A~~B: Security Requirements for Systems Accessing the OPTN Computer System*, as soon as possible, but no later than:
        - 24 hours following the ~~information security contact~~ member 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~~ member becoming aware of the security incident if the member does disconnect the affected users and any impacted systems from the OPTN Computer System
    - Notification to the OPTN Contractor of any privacy incident involving data obtained from the OPTN Computer System, except for data which a member incorporates into a member's own system for candidate, recipient, or donor medical records. Notification must occur as soon as possible, but no later than 48 hours following the member becoming aware of the privacy incident.
    - 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 or privacy 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 or privacy 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~~D.i: Information Security Contact

~~Transplant hospital, organ procurement organization, and histocompatibility laboratory~~ M~~m~~embers 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
2. Receive relevant notifications of security incidents and privacy incidents from the member's information security staff
3. Communicate information regarding security incidents and privacy incidents to the OPTN
4. Facilitate development and fulfillment of OPTN Obligations outlined in *OPTN Policy 3.1.~~A~~B: Security Requirements for Systems Accessing the OPTN Computer System*

Affected OPTN Management and Membership Policies Language[5]

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

F.7: Business Members[6]

A business member must be an organization ~~in operation for at least one year~~ that engages in commercial activities with ~~two~~ one or more active OPTN transplant hospital, OPO, or histocompatibility laboratory members.

A. Business Member Representatives

Business members ~~must indicate membership acceptance by designating in writing to the Executive Director the name of a representative and address to which notices may be sent.~~ have the following responsibilities:

1. Appoint a representative to act for the member on all OPTN business.
2. Appoint an alternate representative who will have authority if the representative is unable to act.
3. Submit in writing to the Executive Director the name and contact information of its representative and alternate representative.

[5] This proposal was originally drafted using the former structure of the OPTN Policies and OPTN Bylaws. On December 2, 2024, the OPTN adopted a new structure of governance, splitting the OPTN Bylaws into two documents: the OPTN Bylaws and OPTN Management and Membership Policies. The references to the affected provisions have been updated to match the format adopted in December. For more information, please see the OPTN proposal *Revised Bylaws and Management and Membership Policies,* available at https://optn.transplant.hrsa.gov/media/vwuovfyu/excom_revised-bylaws-and-management-and-membership-policies_bp.pdf.

[6] Originally located in *OPTN Bylaw 1.7: Business Member*.

Appendix M: Definitions

[…]

Business Members

A membership category of the OPTN. A business member is an organization ~~in operation for at least one year~~ that engages in commercial activities with ~~two~~ one or more active OPTN transplant hospital, OPO, or histocompatibility laboratory members.