OPTN

Briefing to the OPTN Board of Directors on

Revise Conditions for Access to the OPTN Computer System

OPTN Network Operations Oversight Committee

Prepared by: Lindsay Larkin
UNOS Policy Department

Contents

Revise Conditions for Access to the OPTN Computer System

Affected OPTN Policies:	*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*
Affected OPTN[1] Management and Membership Policies:	*6.7: Business Members* *6.7.A: Business Member Representatives* *Appendix M: Definitions*
Sponsoring Committee:	*Network Operations Oversight*
Public Comment Period:	*July 31 – September 24, 2024*
Board of Directors Meeting:	*December 2-3, 2024*

Executive Summary

The Organ Procurement and Transplantation Network (OPTN) Network Operations Oversight Committee (NOOC) proposes strengthening the protections of OPTN data and the OPTN Computer System by revising the conditions for access to the OPTN Computer System in the following ways:

- Require OPTN membership as a condition of access to the OPTN Computer System
- Reduce potential barriers to OPTN business membership
- Limit access to the OPTN Computer System to the following functions: 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 Interconnection Security Agreement (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

[1] This proposal was originally drafted using the former structure of the OPTN Policies and OPTN Bylaws. On July 24, 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 July. For more information, please see the OPTN proposal *Revised Bylaws and Management and Membership Policies,* available at https://optn.transplant.hrsa.gov/media/g1hfngvs/specialpc_invest_combineddoc.pdf.

While the OPTN Computer System has robust measures in place to protect against security incidents, these additional proposed actions further support adherence to National Institute of Standards and Technology (NIST) requirements.[2]

[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).

Purpose

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 ISAs is necessary to adhere to NIST requirements.[3]

Background

The Network Operations Oversight Committee (NOOC) is an operating committee of the OPTN Board of Directors. It assists the OPTN Board in its oversight of the OPTN operations, including the OPTN matching function, the process of official OPTN data collection including data from potential donors, deceased donors, living donors, transplant candidates, and transplant recipients required for the OPTN matching function and other OPTN activities. The NOOC is comprised of OPTN Board members who represent transplant hospitals, organ procurement organizations (OPOs), histocompatibility labs, and the patient community. External subject matter experts with vast backgrounds in information technology and cybersecurity leadership also advise the NOOC.

In June 2023, the OPTN Board approved a proposal to *Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements*.[4] These policy measures increased transplant hospital, OPO, and histocompatibility lab information security by addressing the following:

- Security framework and controls for members with access to the OPTN Computer System
- Self-attestation regarding the member's existing security framework
- Auditing and compliance monitoring for security requirements
- Security requests for information
- Development of an incident response plan, i.e. required actions for a security incident
- Establishment of an information security contact role
- Security training for all OPTN Computer System users

While these policies increased information security for transplant hospital, OPO, and histocompatibility lab members, they did not address security requirements for business organizations accessing the OPTN Computer System. [5] Business organizations often contract with member organizations to provide staffing for functions such as organ donor management, organ placement, and evaluation of organ offers. They only have access to data within the OPTN Computer System that is granted to them by Site Security Administrators at each member organization. For the purposes of information security and

[3] 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).
[4] *Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements*, Briefing to the OPTN Board of Directors. June 2023.
[5] 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 modified the OPTN Contract in August 2022 to require the OPTN Contractor to undertake additional security measures for the OPTN Computer System, including working with the NOOC to establish membership requirements for those members interacting with the OPTN Computer System.

safety of patient data, security requirements must universally apply to all membership categories who access the OPTN Computer System, including business organizations. By requiring membership of all organizations accessing the OPTN Computer System, security requirements will be universally applied across membership categories and uphold information security and safety of patient data.

National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev. 5 Control AC-20 requires the OPTN to establish data use agreements (DUAs) with member organizations to establish terms and conditions that address access to the OPTN from external information systems or process, store, or transmit OPTN data using external information systems. [6] Adherence to NIST SP 800-53 Rev. 5 Control CA-03 requires that the OPTN document, authorize, review, and update ISAs with OPTN member organizations that utilize Application Programming Interfaces (APIs) to access data within the OPTN Computer System. [7] This proposal would require ISAs between the OPTN and every member that interconnects with the OPTN Computer System. A follow-up proposal will address DUA requirements.

Proposal for Board Consideration

This proposal enhances the overarching information security of the OPTN Computer System, OPTN data, and business organizations who use the OPTN Computer System through the following proposed changes:

- 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

In addition, the Committee is proposing a transition period for business organizations to be approved as business members within the OPTN.

Membership as a Condition of Access to the OPTN Computer System

Currently, transplant hospitals, OPOs, and histocompatibility labs can grant non-members permissions to access data within the OPTN Computer System per *OPTN Policy 3.1.D: Non-Member Access*. While OPTN members are required to have a DUA with the non-member, the OPTN is currently not a party to this agreement and has no contractual mechanism to appropriately ensure the safety of data within the OPTN Computer System once it is accessed by the non-member, aside from the overarching system Terms of Use.[8]

[6] 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).
[7] 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).
[8] UNOS Policies & Terms, https://unos.org/privacy-policy/.

This proposal requires that every business organization that requires access to the OPTN Computer System apply for and be granted OPTN business membership in order to be eligible to access the OPTN Computer System.[9] The qualifications, privileges, and requirements of an OPTN business member are described in *OPTN Management and Membership Policy 6.7: Business Members*.[10]

Overall, these requirements enhance system safety and support additional protection of data within the OPTN Computer System. Requiring organizations that access the OPTN Computer System to be OPTN members means they would have to comply with OPTN policies and bylaws, including the stated security standards for OPTN members accessing the OPTN Computer System. These requirements would provide the OPTN with an avenue for increased accountability and oversight regarding access to the computer system.

Overall, public comments supported prioritizing the security of the OPTN Computer System, establishing a pathway for businesses to become OPTN members, and having the same policy standards apply to business members as to all other members.

Revise the Requirements for Business Members[11]

The Committee proposes revising the requirements for OPTN business membership in order to reduce potential barriers for new and small businesses to become OPTN business members by:

- Removing the requirement that the organization has to have been in business greater than one year, in order to allow new businesses to join the OPTN
- Reducing the requirement that the organization be contracted with two or more OPTN members to being contracted with one or more OPTN members, to allow smaller businesses to join the OPTN

In addition to reducing barriers for newer and smaller businesses to become OPTN members, the Committee proposes a requirement for business members to identify an alternate representative. Currently, transplant hospitals, OPOs, and histocompatibility labs require a primary and an alternate representative for contact related to OPTN functions. However, business members are currently only required to have a primary representative without an identified alternate. The goal of this change is to ensure that the OPTN can reach a representative of the organization who could make decisions on behalf of the organization should the need arise, so that there is not a single point of failure.

Public comments generally supported the proposed bylaw changes for business members, though some concerns were noted. There were questions regarding the ability of business members to vote on OPTN matters or serve on OPTN committees, with the majority of comments expressing concern for business members being able to vote on OPTN matters. Current *OPTN Management and Membership Policy 6.1.B: Overview of Voting Process*[12] and *6.7.C: Business Membership Voting Privileges*[13] both state "Business members do not have voting privileges in the OPTN". This proposal does not change either of

[9] *OPTN Management and Membership Policy Appendix A: Membership Application and Review*.
[10] Originally located in *OPTN Bylaw 1.7: Business Members.*
[11] This proposal was originally drafted using the former structure of the OPTN Policies and OPTN Bylaws. On July 24, 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 July. For more information, please see the OPTN proposal *Revised Bylaws and Management and Membership Policies,* available at https://optn.transplant.hrsa.gov/media/g1hfngvs/specialpc_invest_combineddoc.pdf.
[12] Originally located in *OPTN Bylaw 1.1.B: Overview of Voting Process.*
[13] Originally located in *OPTN Bylaw 1.7.C: Business Membership Voting Privileges.*

these provisions nor does it add a requirement for business member representation on OPTN committees. All committee representatives are selected based on background, expertise, and an evaluation of any conflict of interest. If an individual employed by a business member happens to be selected to serve on an OPTN committee, they are permitted to vote on the committee's business (so long as there is no conflict of interests according to *OPTN Management and Membership Policy 4.3: Conflicts of Interest*).[14]

Additionally, some comments questioned whether there is a fee associated with OPTN business membership. The Committee clarified the intention of the proposal is for the OPTN to exercise authority over a business member's access to the OPTN Computer System and there are no fees associated with membership to the OPTN, which is consistent across all member types.

Business Member Users within the OPTN Computer System

All businesses are reviewed by the OPTN Contractor prior to access credentialing. This review includes confirming that the reasons for access are permissible and meet current OPTN policy requirements. The business must have an active contract with an OPTN member. Additional reviews by the OPTN Contractor are conducted throughout the year to ensure access is still needed and the business still meets all requirements.

A few public comments expressed concern that granting access to a broader group of organizations could increase risk to the system. The Committee discussed this concern and reiterated the intent of the proposal is to ensure business organizations, some of whom already access the OPTN Computer System, become business members who are held to the same security standards as all other OPTN members to enhance system safety and support additional protection of data within the OPTN Computer System. Some comments suggested limiting the types of businesses eligible for OPTN membership or defining different "tiers" of external business partners to restrict their scope of access based on their support functions. The Committee discussed this feedback and clarified business members will only have access to data based on the permissions granted by transplant hospitals, OPOs, or histocompatibility laboratories with whom they are contracted with. According to OPTN Policy *3.1.B: Site Security Administrators*, site administrators at transplant hospitals, OPOs, and histocompatibility laboratories are routinely required to audit the permissions of all users in their purview, which includes users at business organizations, and permission levels must be granted according to the NIST principle of least privilege.[15] The Committee also plans to discuss further oversight of business members as part of a future project.

Permissible Reasons for Access to the OPTN Computer System

This proposal outlines the authorized purposes for accessing the OPTN Computer System for OPTN members, including transplant hospitals, OPOs, histocompatibility labs, and business members. Previously, authorized purposes for member access were not clearly specified in policy.

The most integral reason for any member to access the OPTN Computer System is to facilitate organ transplantation. Organ transplantation is facilitated by entering or managing candidate or donor data; offering organs, evaluating organ offers, and responding to organ offers; or providing transportation and

[14] Originally located in *OPTN Bylaw 2.8: Conflicts of Interests*.
[15] "The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function." NIST SP 800-53 Rev. 5.

logistical support for getting the organ from the donor to the candidate. In order to leave room for post-transplant follow-up data submission and any future OPTN requirements, the Committee is also proposing that "fulfilling OPTN obligations" as defined in *OPTN Management and Membership Policy Appendix M: Definitions* be included in the reasons for any member to access the OPTN Computer System.[16] One public comment suggested clarifying the term "facilitating organ transplantation" to include post-transplant follow-up of donor data. The Committee agreed with the comment and will include clarifications within the implementation education for members.

The Committee also proposes that quality assurance and performance improvement (QAPI) measures are acceptable reasons for transplant hospitals, OPOs, and histocompatibility labs to access the OPTN Computer System. The Health Insurance Portability and Accountability Act (HIPAA) includes "conducting quality assessment and improvement activities" in their definition of health care operations.[17] According to HIPAA, "A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information", and in accordance with this provision the OPTN discloses data to transplant hospitals, OPOs, and histocompatibility labs for QAPI purposes.[18]

This proposal prohibits any organization from accessing the OPTN Computer System for research purposes. The OPTN is required to make data available to researchers, and does so through other processes external to the OPTN Computer System, in order to ensure compliance with relevant security and privacy requirements, as well as the OPTN Final Rule.[19] For example, the OPTN Final Rule requires that "Patient-identified data may be made available to bona fide researchers upon a showing that the research design requires such data for matching or other purposes, and that appropriate confidentiality protections, including destruction of patient identifiers upon completion or matching, will be followed."[20] This means that the OPTN cannot provide access to such patient-identified data without ensuring that researchers have appropriate protections in place.

If patient-identified data is required for research, the OPTN is required to provide it via the patient-identified data request pathway, which ensures adherence to all regulations under HIPAA and the OPTN Final Rule. [21,22] The OPTN data request pathway requires that the OPTN processes research requests expeditiously, "with data normally made available within 30 days from the date of the request".[23] Requests via the patient-identified data request pathway require a data use agreement (DUA), security plan, research plan, and an approved institutional review board (IRB) protocol or IRB exemption to be submitted to HRSA for approval. Requests for de-identified limited data sets or aggregated data, either standard or custom, follow a similar data request process.[24]

Furthermore, while the OPTN is required to "Provide data to an OPTN member, without charge, that has been assembled, stored, or transformed from data originally supplied by that member", the OPTN

[16] Originally located in *OPTN Bylaw Appendix M: Definitions*.
[17] 45 CFR §164.501.
[18] 45 CFR §164.506(c)(4).
[19] Department of Health and Human Services 42 CFR Part 121 Organ Procurement and Transplantation Network; Final Rule (63 Federal Register 16295, at 16332, April 2, 1998).
[20] 42 CFR §121.11(b)(1)(v).
[21] 45 CFR §164.512 (i).
[22] 42 CFR §121.11(b)(1)(v).
[23] 42 CFR §121.11(b)(1)(v).
[24] OPTN Data Request Instructions: https://optn.transplant.hrsa.gov/data/view-data-reports/request-data/data-request-instructions/.

Computer System is not the appropriate vehicle for the provision of this data, as the OPTN must still ensure all relevant security and privacy measures are in place to protect the data once released back to the member. [25]

Some public comments expressed concerns about the limitations on access to the OPTN Computer System for research purposes. They urged that the data request process remain straightforward and not overly burdensome. The Committee discussed this concern and clarified the proposal does not include any changes to the current data request pathway, nor does the proposal impact current access to Standard Transplant Analysis and Research (STAR) files or Scientific Registry of Transplant Recipients (SRTR) reports.[26]

Reporting Privacy Incidents

The current OPTN security incident management policies require OPTN member reporting of security incidents in the computing environments and components thereof which are used to access the OPTN Computer System. These requirements also extend to associated environments used to manage the OPTN member's computing environment used to access the OPTN Computer System. Such associated environments include system-administrator-level accounts or systems, which would manage accounts or environments used to access the OPTN Computer System. However, if a system is fully segmented, such as into clinical care and research, only the segments used to access the OPTN Computer System, or manage those segments, would be included.

This proposal adds additional reporting requirements for privacy incidents. Incidents involving any data obtained from the OPTN Computer System must be reported to the OPTN by OPTN members. This does not mean that any privacy incident involving a member's data on a transplant candidate would need to be reported. But, as proposed, if there is an incident related to any data the OPTN member has obtained via the OPTN Computer System or through a research request that is stored in the member's systems (such as on the member's electronic medical records [EMRs]), the member must report the incident to the OPTN within 48 hours following the member becoming aware of the privacy incident. This includes data related to deceased organ donors and organ offers. In addition, the member must report to the OPTN if a member downloaded and stored any data from the OPTN Computer System that was involved in a privacy incident. Public comments endorsed the proposed privacy incident reporting requirements.

Interconnection Security Agreements (ISAs)

An ISA is "a document specifying information security requirements for system interconnections, including the security requirements expected for the impact level of the information being exchanged for all participating systems."[27] Currently, the OPTN provides Application Programming Interfaces (APIs) as the only method for interconnection to the OPTN Computer System for data exchange. If this policy is approved, all of these organizations will be required to execute an ISA with the OPTN in order to maintain API connections to the OPTN Computer System, and future connections will require an ISA prior to being activated.[28] Organizations that do not integrate with the OPTN Computer System via API

[25] 42 CFR §121.11(b)(1)(vii).
[26] STAR (Standard Transplant Analysis and Research) files are datasets that contain de-identified patient-level information for transplant recipients and waiting list candidates back to 10/1/1987.
[27] National Institute of Standards and Technology (NIST) Special Publication 800-47 Revision 1: Managing the Security of Information Exchanges. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-47r1.pdf. (July 2021).
[28] See Appendix A: Sample Interconnection Security Agreement (ISA) Template and Language.

will not be required to execute an ISA with the OPTN. Organizations will only be required to execute one ISA per connected member system. Therefore, if the member only connects via a single EMR at their organization, only a single ISA would be required, even if that EMR serves multiple OPTN members.[29] The OPTN Computer System is required to adhere to NIST SP 800-53 Revision 5 for its Authority to Operate (ATO), which includes remediation of all security findings within a specified timeframe.[30] The ATO requires the OPTN to authorize, review, and update Interconnection Security Agreements (ISAs) with OPTN member organizations utilizing APIs to access data within the OPTN Computer System.[31] NIST guidance recommends that an ISA should be established "whenever the security policies of the interconnected systems are not identical, and the systems are not administered by the same Authorizing Official (AO)".[32] An ISA documents the security protections that must operate on interconnected systems to ensure that transmission between systems permits only acceptable transactions. It also formalizes the security understanding between the authorities responsible for the electronic connection between the systems.[33] It authorizes mutual permission to connect both parties and establishes a commitment to protect data that is exchanged between the networks or processed and stored on systems that reside on the networks. It minimizes the susceptibility of connected systems and networks to information security risks and aids in the mitigation and recovery from information security incidents.

ISAs are different from existing member security attestations, as security attestations only assess the current state of member security frameworks on a by-control basis. Security attestations do not agree to minimum security standards, nor describe system interconnections. ISAs are also different from Data Use Agreements (DUAs). DUAs are an agreement for how shared data can be used, while an ISA is a security document describing and developing security standards for system interconnections.

The OPTN Contractor will be providing the ISA template to the members' Information Security Contact(s), who will have the ability to reassign the ISA to any individuals at their organization who need to develop, review, or sign. While members can request changes to provisions within the ISA, such requests are contingent upon NOOC review and approval.

ISAs will be required to be renewed every three years, which is the maximum timeframe allowed by NIST SP 800-53 Rev. 5 guidance.[34] Centers for Medicare and Medicaid Services (CMS) currently requires annual review of their ISAs.[35] When discussing the timeframe for renewal of OPTN ISAs, the Committee felt that ISAs require significant effort for members to develop and felt that the maximum timeframe was appropriate. In addition, the Committee is proposing that members are required to update their ISAs with every change to the information contained within the ISA to ensure the ISAs contain current information. Public comments recommended there also be a time constraint applied to the requirement

[29] 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).
[30] 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).
[31] HRSA FND-2387 – ISA (Interconnection Security Agreement). HHS Contract # HHSH250201900001C.
[32] National Institute of Standards and Technology (NIST) Special Publication 800-47 Revision 1: Managing the Security of Information Exchanges. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-47r1.pdf. (July 2021).
[33] Committee on National Security Systems (CNSS) Committee on National Security Systems (CNSS) Glossary, CNSS Instructions (CNSSI) No. 4009. https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf. (March 2, 2022).
[34] 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).
[35] Centers for Medicare and Medicaid Services (CMS) CMS Security and Privacy Agreement Guidance. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/CMS-Data-Agreement-Guidance.pdf.

to complete initial ISA agreements. The Committee agreed with this recommendation and added language to the policy to require ISA agreements be completed within six months of being issued by the OPTN.

Business Member Information Security Requirements

The Committee developed information security requirements that apply to transplant hospitals, OPOs, and histocompatibility labs in a previous proposal that was approved by the OPTN Board of Directors in June 2023.[36] This proposal is intended to further secure the OPTN Computer System by creating the same security requirements for business members who access the OPTN Computer System. These requirements do not apply to business members who do not access the OPTN Computer System.

As stated above, public comments supported prioritizing the security of the OPTN Computer System and establishing a pathway for businesses to become OPTN members, with the expectation that the same requirements apply to business members as to all other members. Some comments did express concern for the burden placed on members to complete the security requirements established in the Committee's previous *Establishing Member System Access, Security Framework, and Incident Management and Reporting Requirements* proposal. Commenters cautioned the Committee to ensure that these requirements do not disrupt patient care and to ensure the overall administrative load on users should be minimized to maintain system efficiency. A specific area of concern was the proposed requirement for site access administrators to remove a user's access to the OPTN Computer System no later than 12 hours after their user's last day of employment or there is a change in a user's role or responsibilities. Commenters stated this timeframe was too burdensome and requested the requirement be adjusted to no later than 24 hours. The Committee agreed with the comment and changed the proposed policy language.

Information Security Contact

This proposal requires business members to identify an Information Security Contact.[37] This role is intended to be the individual responsible for compliance with the OPTN security requirements, as well as the point of contact for the OPTN for self-attestations, audits, security requests for information, and security incident reporting. The member must also have internal policies to ensure that the Information Security Contact is notified of declared security incidents.

The public comment proposal included additional language that required the Information Security Contact "who fulfills an active information security role at the member organization". This language would apply to **all** OPTN members, and therefore would have required all members to audit their identified Information Security Contacts to ensure they meet this new requirement. A key theme throughout the public comments received was for the Committee to ensure the proposal does not add undue burden on OPTN members to meet the new requirements. Therefore, the Committee decided to remove this proposed language from the final policy and will revisit specific roles outlined in policy as needed.

[36] *Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements*, Briefing to the OPTN Board of Directors. June 2023.
[37] *OPTN Policy 3.1.C.i: Information Security Contact*.

Security Framework and Controls

Business members will also be expected to, at a minimum, follow all the NIST SP 800-171 framework controls. [38] Members who are compliant with other security frameworks must still show that all 110 controls required by NIST SP 800-171 are covered in an annual attestation. Due to the vast array of potential solutions for each control, this proposal does not dictate how to operationalize these controls. Each member will develop their solution based on their current level of information security maturity and their own functional needs.

Attestations

This proposal includes a requirement for business members to submit an annual self-attestation stating their compliance with the NIST SP 800-171 security framework or equivalent. Once implemented for business members, attestations will be distributed annually or upon request by the OPTN. New business members will be provided with attestations to complete before they are granted access. Members will have 90 days to complete their attestations after it is assigned to them.

Calls for attestation will be distributed to the Information Security Contact with instructions for completion and return. The first attestation will be a readiness assessment, evaluating only critical- and high-risk controls as defined by NIST SP 800-171 Rev 2, which total 58 out of the 110 controls. Members may not be immediately able to attest to full compliance with all security controls upon implementation of this proposal. Members would be expected to specify which controls they do and do not adhere to in the initial attestation and work with the OPTN Contractor's information security team to manage and remediate the risks associated with non-compliance.

Routine Audits

The Committee is proposing that business members also be subject to security audits every three years. The auditing criteria will be compliance with the controls from NIST 800-171. These audits will begin after sufficient time for members to implement a security framework and act on their Plans of Action and Milestones (POAMs) for any controls that are not yet implemented.

Security Requests for Information

In order to ensure that known exploited vulnerabilities with the potential to impact the OPTN Computer System have been addressed by members, the OPTN may perform security requests for information (RFIs). These requests for information inform the OPTN of the state and remediation status of the vulnerability within the member's environment. These requests will be distributed after Cybersecurity and Infrastructure Security Agency (CISA) notification of a critical or high known exploited vulnerability, to ensure that the risk has been addressed. The timing for required response to these requests for information will be based on the level of threat of the vulnerability, as defined by the Department of Homeland Security. [39]

---

[38] National Institute of Standards and Technology (NIST) Publication 800-171 Revision 3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf. (May 2024).

[39] Cybersecurity and Infrastructure Security Agency. (2019). *BOD 19-02: Vulnerability remediation requirements for internet accessible systems.* U.S. Department of Homeland Security.

Security Incidents and Response

This proposal maintains the OPTN definition of a security incident, which is "[a]n event that is declared as jeopardizing the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits."[40] It only encompasses declared security incidents, not every potential incident under investigation by a member, as well as security incidents involving those machines and devices that are used to access or manage access to the OPTN Computer System. This proposal requires that business members now also develop and comply with an incident response plan, to be available to the OPTN upon request.

In the event of a security incident, 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. This may include on-site remediation with oversight by the OPTN Contractor and/or requiring the member to disconnect from the OPTN Computer System until the OPTN has determined the risk is mitigated. Members will be required to meet control and verification requirements as provided by the NOOC based on the type of security incident. These requirements will be communicated directly to the member through the information security points of contact established in the member's incident response plan.

The OPTN Contractor has response procedures in place and will need to investigate the scope of the compromise to determine potential impacts to other members and determine if there is any indication of compromise to OPTN systems. The response to the incident will be based on the type of security incident and level of compromise. Mitigation and containment will prioritize ensuring minimal impact to transplantation, through new secure systems access if endpoints are compromised at the member institution.

This proposal will not change existing OPTN security incident notification requirements. The OPTN Contractor is required to notify HRSA within one hour of a declared security incident, and to follow HRSA's direction regarding any additional notifications.[41]

Transition Procedures

The Committee recognizes that many of the proposed requirements require a transition period for members, as some requirements are dependent on others being implemented. The Committee is proposing an 18-month transition period to fully implement all portions of this proposal, apart from member security audits. Member security audits will be implemented at the same time for all member types.[42] Reporting of privacy incidents involving data obtained from the OPTN Computer System will be required for all member types after approval of this proposal.

Business Membership

Upon implementation, business organizations who access the OPTN Computer System will be provided with a 90-day timeframe to apply for OPTN business membership if they are not already members. This

[40] *OPTN Policy 1.2: Definitions*.
[41] OPTN Contract, HHSH250201900001C, Performance Work Statement (PWS) Task *3.20.4: Incident Response*.
[42] Transplant hospital, Organ Procurement Organization, and Histocompatibility Laboratory member security audits are already required by the proposal *Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements*, which was approved by the OPTN Board in June 2023.

will be followed by a one- to two-month review period by the MPSC, after which organizations will be granted interim business membership if they meet all conditions within the proposed *OPTN Management and Membership Policy 6.7: Business Members*. After interim approval, the member may function as an OPTN member while awaiting review by the OPTN Board.[43]

All business members, regardless of OPTN Computer System access, will need to submit the name of an alternate representative under the proposed revised bylaw. Business members will have 90 days to submit the name and contact information for their alternate representative.

All business organizations with access to the OPTN Computer System who are not business members will be notified prior to the beginning of the 90-day application period, and OPTN Computer System access will be removed for any organization who does not apply within that period.

Review of Permissible Reasons for Access to the OPTN Computer System

Concurrently with the business membership transition process, the OPTN will be reviewing permissible reasons for access to the OPTN Computer System. Any business member who is not facilitating transplantation or assisting a member with fulfilling OPTN obligations in line with the proposed policies, will have their OPTN Computer System access removed. All business organizations with access to the OPTN Computer System will be contacted at the beginning of the review period and will have 90 days to submit their reasons for access. The NOOC will review permissible reasons for access and vote on recommended course of action for each business member based on alignment with policy.

Business Member Reporting of Information Security Contacts, Security Incidents, and Response to Requests for Information

As part of business member applications, organizations applying to be business members will be asked to provide the name and contact information for their Information Security Contact(s) (ISCs). Upon approval of interim business membership, business members will be required to begin reporting security incidents in systems that connect to the OPTN Computer System. They will also be required to respond to any information security requests for information (RFIs).

Business Member Attestations

The OPTN Contractor will send member security attestations to all ISCs at business members who access the OPTN Computer System. Business members will have 90 days to complete the security attestations, which aligns with the current requirements for transplant hospitals, OPOs, and histocompatibility labs. The attestation will consist of questions on the implementation status of the 58 critical- and high-risk security controls from NIST 800-171 Rev. 2. All active business members who access the OPTN Computer System will be assigned the security attestation.

Obtaining ISAs

The OPTN Contractor will send ISA templates to information security contacts at all OPTN members that connect to the OPTN Computer System via API. Members will have six months to complete the ISA agreements once issued by the OPTN Contractor.

---

[43] *OPTN Management and Membership Policy A.1.C: MPSC Review of the Completed Membership Application* as of October 14, 2024.

Next Steps

The NOOC continues to evolve member security requirements to enhance system safety and support additional protections of OPTN data. The Committee will be releasing a follow-up proposal which will require all members who access the OPTN Computer System to execute a DUA with the OPTN.[44] To help develop this proposal, the Committee requested community feedback on necessary DUA requirements which will be reviewed and considered for the DUA proposal development. The Committee has also discussed further clarification for roles and responsible parties within OPTN policy as it relates to security requirements, and further oversight of business member access to the OPTN Computer System as focuses for future projects.

Overall Sentiment from Public Comment

Participation

The proposal was released for public comment from July 31 to September 24, 2024. It received 238 responses out of a total of 1,182 responses received on all projects out for public comment this cycle. Respondents were able to participate through in-person/virtual regional meetings, committee meetings, and a form on the OPTN website. Demographic information was collected from all respondents, including state of origin and stakeholder represented.[45] The comments received represented at least 43 states across the country and all member types, with the greatest participation coming from regional meetings and transplant programs.[46] It is important to consider the demographics participating in the public comment relevant to this proposal thereby ensuring the ultimate recommendation to the Board represents all stakeholders, even those whose volume of participation may be lower. The substance of each comment should be considered, with the volume of comments as a factor but not dispositive of the opinions represented.

Sentiment in Public Comment

Sentiment is collected on public comment proposals, and is measured on a 5-point Likert scale from strongly oppose to strongly support (1-5). **Figure 1** shows sentiment received from all respondents (regional meeting, online, and email) by their self-identified member type. Again, there was overall support for the proposal, demonstrated by a sentiment score of 4.1. **Figure 2** shows sentiment by region. Overall, public comment sentiment was supportive of this proposal, as indicated by the total sentiment score of 4.1 by member type and 4.1 by region, with some pockets of concern as outlined in the sections above.

[44] A Data Use Agreement is an "executed agreement between a data provider and a data recipient that specifies the terms under which the data can be used". National Institute of Standards and Technology (NIST) Publication NISTIR 8053: De-Identification of Personal Information. https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf. (October 2015).
[45] Respondents at regional meetings represent the perspective of an institution, therefore their demographic information represents that of the institution and not the individual submitting the comment.
[46] Most attendees at regional meetings are transplant programs which accounts for the large volume of sentiment scores from transplant programs.

Figure 1: Sentiment by Member Type

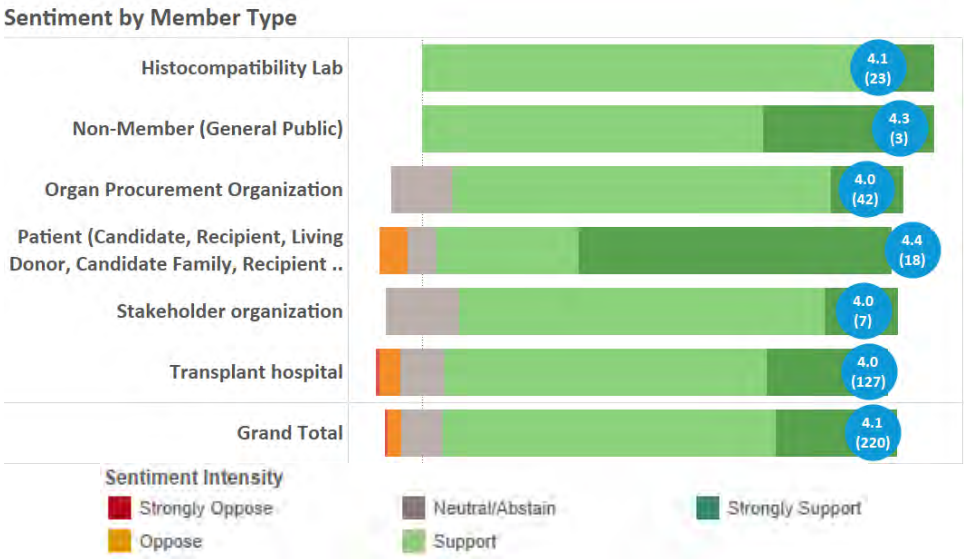
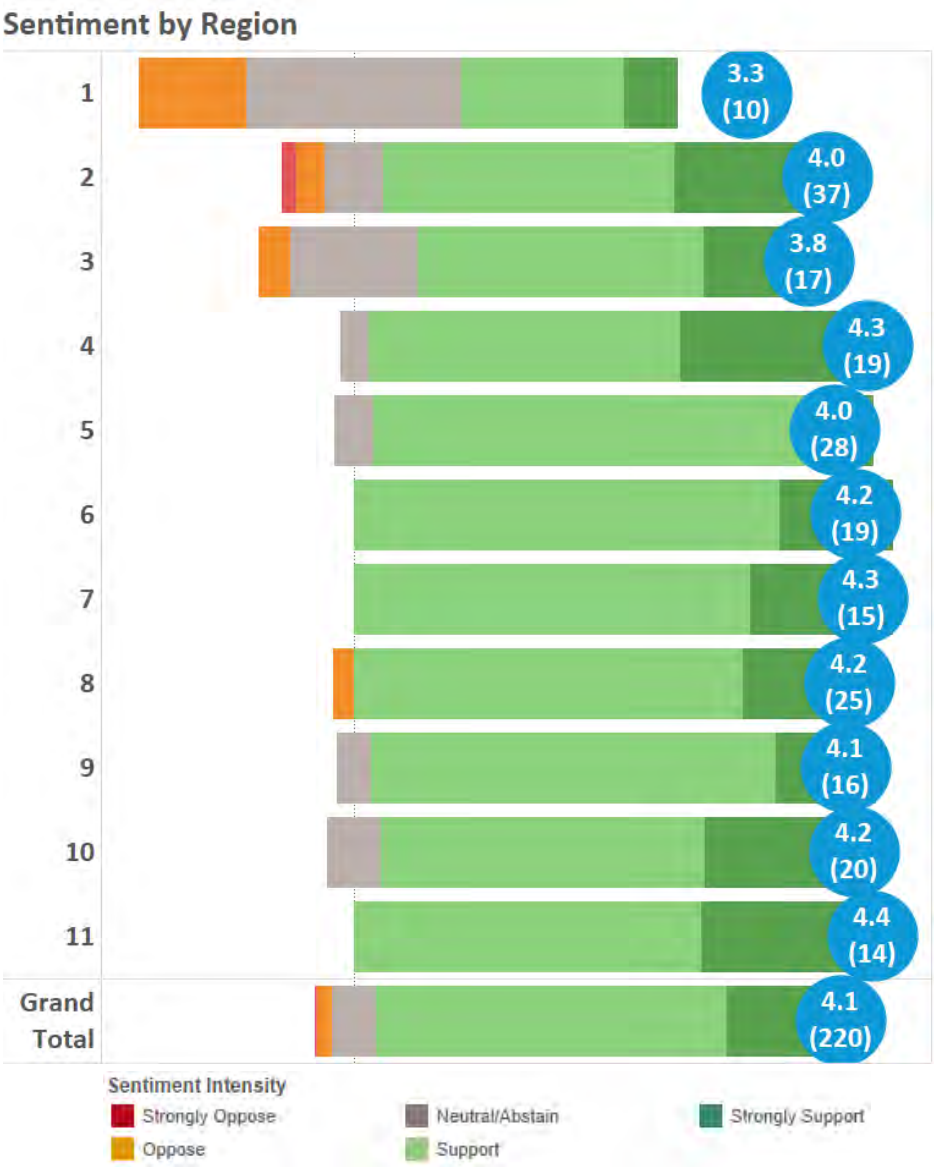


Figure 2: Sentiment by Region



Compliance Analysis

NOTA and OPTN Final Rule

This proposal is provided under the authority of the National Organ Transplant Act of 1984 (NOTA) and the OPTN Final Rule. NOTA requires the OPTN to establish "a national system, through the use of computers and in accordance with established medical criteria, to match organs and individuals included in the list…,"[47] and the OPTN Final Rule requires the OPTN to develop "Policies on such other matters as the Secretary directs."[48] To ensure adherence to NIST requirements, the Secretary has directed the development of OPTN policies to secure the OPTN Computer System, including to require DUAs with

[47] 42 USC §274(b)(2)(A)(ii).
[48] 42 CFR §121.4(a)(6).

every organization that accesses the OPTN Computer System, and ISAs with every organization that interconnects with the OPTN Computer System.

OPTN Strategic Plan[49]

The proposal is aligned with the following OPTN Strategic Plan goal:

- *Support OPTN Modernization Initiatives*: This proposal improves OPTN technology systems by strengthening the protections of OPTN data and the OPTN Computer System.

Implementation Considerations

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 six 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 Members

Operational Considerations

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.[50] 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.

[49] OPTN Executive Committee. Briefing to the OPTN Board of Directors on Strategic Plan 2024-2027. June 2024. Available at: https://optn.transplant.hrsa.gov/media/h51awrli/exec-strategic-plan-briefing-paper.pdf.
[50] National Institute of Standards and Technology (NIST) Publication 800-171 Revision 3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf. (May 2024).

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.

Fiscal Impact

The Fiscal Impact Group (FIG), comprised of representatives from histocompatibility laboratories, organ procurement organizations, and transplant hospitals, reviewed this proposal and completed a survey to estimate anticipated costs. The FIG rates projects as low, medium, or high based on the estimated staffing and/or training, overtime, equipment, or IT support needed in the implementation of this proposal. Based on those factors, the FIG cannot make an assessment of the potential fiscal impact to business members, though it was identified that the costs to business members could also be distributed across clients such as transplant hospitals, organ procurement organizations, or histocompatibility labs and as such would reflect an overall increase in ongoing costs of operations.

Histocompatibility Laboratories

Operational Considerations

All members will now be required to report privacy incidents involving data obtained from the OPTN Computer System. If a member's computer systems connect to the OPTN Computer System, they will be required to complete ISAs every three years and update them 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.

Fiscal Impact

This proposal is not anticipated to have a fiscal impact on histocompatibility laboratories.

Organ Procurement Organizations

Operational Considerations

All members will now be required to report privacy incidents involving data obtained from the OPTN Computer System. If a member's computer systems connect to the OPTN Computer System, they will be required to complete ISAs every three years and update them 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.

Fiscal Impact

This proposal is not anticipated to have a fiscal impact on OPOs.

Transplant Programs

Operational Considerations

All members will now be required to report privacy incidents involving data obtained from the OPTN Computer System. If a member's computer systems connect to the OPTN Computer System, they will be required to complete ISAs every three years and update them 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.

Fiscal Impact

This proposal is not anticipated to have a fiscal impact on transplant hospitals.

OPTN

Operational Considerations

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.

This proposal may require the submission of official OPTN data that are not presently collected by the OPTN or collected in a different format. The OPTN Contractor has agreed that data collected pursuant to the OPTN's regulatory requirements in §121.11 of the OPTN Final Rule will be collected through Office of Management and Budget (OMB) approved data collection forms. Therefore, the modifications to the data collection may be submitted for OMB approval under the Paperwork Reduction Act of 1995.[51]

Fiscal Impact

It is estimated that $31,672 would be needed to implement this proposal. Implementation would involve updates to the Evaluation Plan and the OPTN Computer System, reviewing and preparing implementation communications and educational materials, and answering member questions. In addition, implementation would include routine updates to the NOOC through the implementation period. It is estimated that $1,699,234 will be needed for ongoing support. For the first-year post-implementation, it is estimated $1,123,200 would be needed to cover costs associated with Information Security staff and Information Technology personnel to review business member attestations, business member audits, and interconnection security agreements for all members. It is estimated that $561,600 would be needed to continue this work into the second-year post-implementation. Ongoing support also includes continuing to lead the NOOC through monitoring the policy change and ensure that policy is operating as expected; this will happen through leadership and project management calls and committee meetings. In addition, ongoing support will include consulting on monitoring challenges, consulting on member questions, facilitation of meetings to evaluate and monitor data and any need for

[51] Paperwork Reduction Act of 1995, Pub. L. 104-13 (1995).

further policy development. The total for implementation and ongoing support is estimated to be $1,730,905.[52]

Post-implementation Monitoring

Member Compliance

This proposal includes member monitoring and compliance through the NOOC and OPTN Contractor's information security staff. Member self-attestations will be reviewed for compliance with required controls, and members will receive information security audits every three years. Members must complete their ISAs within six months of OPTN request, renew them every three years, and update it as connected systems, security, and interconnections change. Members must report all qualifying security incidents, and respond to RFIs from the OPTN Contractor. In addition to the compliance monitoring outlined above, all elements required by policy may be subject to OPTN review, and members are required to provide documentation as requested.

Conclusion

This proposal is intended to enhance the overarching security of the OPTN Computer System, OPTN data, and the security of business organizations who use the OPTN Computer System through multiple proposed requirements. The requirements address 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

[52] Resource estimates are calculated by the current contractor for that contractor to perform the work. Estimates are subject to change depending on a number of factors, including which OPTN contractor(s) will be performing the work, if the project is ultimately approved.

OPTN Policy Language[53]

Proposed new language is underlined (example) and language that is proposed for removal is struck through (~~example~~). Heading numbers, table and figure captions, and cross-references affected by the numbering of these policies will be updated as necessary.

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*.[54] Business members may be granted access to the OPTN Computer System for the purposes of facilitating organ 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.

[53] This proposal was originally drafted using the former structure of the OPTN Policies and OPTN Bylaws. On July 24, 2024, the OPTN adopted a new structure of governance, splitting the OPTN Bylaws into two documents: the OPTN Bylaws and the OPTN Management and Membership Policies. The references to the affected provisions have been updated to match the format adopted in July. For more information, please see the OPTN proposal *Revised Bylaws and Management and Membership Policies,* available at https://optn.transplant.hrsa.gov/media/g1hfngvs/specialpc_invest_combineddoc.pdf.

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

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 six months of being issued by the OPTN, reviewed annually, and renewed every 3 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.*[55]
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
    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

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

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*

OPTN Management and Membership Policies Language[56]

Proposed new language is underlined (example) and language that is proposed for removal is struck through (~~example~~). Heading numbers, table and figure captions, and cross-references affected by the numbering of these policies will be updated as necessary.

6.7: Business Members[57]

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.

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.

#

[56] This proposal was originally drafted using the former structure of the OPTN Policies and OPTN Bylaws. On July 24, 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 headers and numbering of the affected provisions have been updated to match the format adopted in July. For more information, please see the OPTN proposal *Revised Bylaws and Management and Membership Policies,* available at https://optn.transplant.hrsa.gov/media/g1hfngvs/specialpc_invest_combineddoc.pdf.

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

Appendix A: Post-Public Comment Changes

New language that was proposed following public comment is underlined and highlighted (example); language that is proposed for removal following public comment is struck through and highlighted (~~example~~).

Excerpts from *OPTN Policy*[58]

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 six months of being issued by the OPTN, reviewed annually, and renewed every 3 years.

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 ~~12~~ 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 ~~12~~ 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

[58] This proposal was originally drafted using the former structure of the OPTN Policies and OPTN Bylaws. On July 24, 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 July. For more information, please see the OPTN proposal *Revised Bylaws and Management and Membership Policies,* available at https://optn.transplant.hrsa.gov/media/g1hfngvs/specialpc_invest_combineddoc.pdf.

- 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 ~~12~~ 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.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 fulfills an active information security role at the member organization. The information security contact~~ who is responsible for maintaining and complying with a written protocol that includes how an information security contact will:

[…]