ISHLT
A Society that Includes Basic Science, the Failing Heart, & Advanced Lung Disease

ISHLT Response to OPTN Revise Conditions for Access to the OPTN Computer System

The International Society for Heart and Lung Transplantation (ISHLT) appreciates the opportunity to provide feedback on the "Revise Conditions for Access to the OPTN Computer System and Reporting Privacy Incidents involving OPTN Data" OPTN public comment.

ISHLT reviewed the OPTN's proposal, which focuses on revising membership requirements and enhancing security protocols for accessing OPTN computer systems. The proposal is intended to ensure that entities supporting transplant centers, OPOs, and histocompatibility laboratories access the OPTN system in a manner that safeguards data privacy and security, consistent with NOTA and the OPTN Final Rule. The proposal outlines security requirements for members utilizing APIs to access OPTN data.

ISHLT has concerns regarding the potential limitations on third-party access to OPTN data for research purposes, as well as the impact these restrictions might have on current research pathways.

ISHLT also has concerns that the description of "Interconnection Security Agreements" (ISAs) lacks clarity whether there are circumstances where the vendors who supply the software platforms (such as EHRs) members use to access APIs must be parties to these agreements.

ISHLT Responses to the OPTN Considerations for the Community questions are as follows:

Bylaw Changes for OPTN Membership (Small and New Businesses)
ISHLT supports the proposed bylaw changes, provided that high security standards and compliance measures are upheld.

Feasibility of the Transition Plan
The feasibility of the transition plan will depend on expert analysis to ensure a realistic timeline, adequate resources, and minimal disruption to clinical and research operations.

Additional Obstacles to Completing the Transition Plan
Potential obstacles include challenges with system interoperability, increased compliance burdens, limitations on research access, and cost implications.

Data Use Agreement (DUA) Recommendation
The DUA should set clear expectations for data integrity, accuracy, and HIPAA compliance. It must define privacy parameters for authorized users and set limitations on third-party use of OPTN data. The agreement should include breach notification requirements, clarify data ownership, and specify the consequences for non-compliance, as well as dispute resolution mechanisms.

In conclusion, ISHLT supports the OPTN proposal while emphasizing the need to refine key details to balance security with accessibility. Ensuring that security and data access changes do not impede legitimate research is paramount. Changes should not place significant burdens on clinicians and researchers. Ensuring resources and training are readily available will be critical.

We recommend refining the draft to clarify the parties required for ISAs and address security implementation details. We also recommend that the proposal include clear guidelines on shared responsibilities between hospitals, vendors, and the OPTN to avoid ambiguity, ensuring research pathways, particularly for donated organs not utilized for transplantation, remain accessible despite the new restrictions.

ISHLT Level of Support: Support the Policy

OPTN

Public Comment Proposal

Revise Conditions for Access to the OPTN Computer System

OPTN Network Operations Oversight Committee

Prepared by: Courtney Jett
UNOS Policy Department

Contents

Revise Conditions for Access to the OPTN Computer System and Reporting Privacy Incidents

Affected 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 Bylaws:	*1.7: Business Members* *1.7.A: Business Member Representatives* *Appendix M: Definitions*
Sponsoring Committee:	*Network Operations Oversight*
Public Comment Period:	*July 31 – September 24, 2024*

Executive Summary

The 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 develop an Interconnection Security Agreement (ISA) with 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

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.[1]

[1] 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

The goal of this proposal is 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, many of whom are third party contractors, who access the computer system. Enhancing the security of the OPTN Computer System protects candidate, recipient, and donor data, and increases public trust. Furthermore, the institution of OPTN ISAs are necessary to ensure adherence to NIST requirements.[2]

Background

In June 2023, the OPTN Board of Directors passed a proposal to *Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements*.[3] These policies developed measures to increase 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 attained increased information security for transplant hospital, OPO and histocompatibility lab members, they did not address requirements for business organizations within the OPTN Computer System.[4] As of May 2024, there were 38 business organizations with access to the OPTN Computer System, and 702 users whose primary affiliation is with a business organization. Business organizations are not currently required to be members of the OPTN, with only 29 percent of those business organizations opting for OPTN business membership.[5] For the purposes of information security and safety of patient data, security requirements must universally apply to all membership categories who access the OPTN Computer System, including business organizations.

Adherence to National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev. 5 Control AC-20 requires the OPTN to establish DUAs with member organizations to establish terms and conditions that address access to the OPTN from external information systems or process, store, or

[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).
[3] *Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements*, Briefing to the OPTN Board of Directors. June 2023.
[4] 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.
[5] Based on OPTN Data as of May 1, 2024.

transmit OPTN data using external information systems.[6,7] 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.[8,9] 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.

Overview of Proposal

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 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 develop an ISA with 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 membership 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 use the OPTN Computer System per OPTN *Policy 3.1.D: Non-Member Access*. While members are required to have a DUA with the non-member, the OPTN is currently a third-party to this agreement and has no mechanism to appropriately ensure the safety of data within the OPTN Computer System once it is accessed by the non-member.

This proposal would allow all current business organizations who have appropriate reasons for access to the OPTN Computer System (see *Reasons for Access to the OPTN Computer System*) to apply for and receive business membership through a standard membership application. As of May 2024, there were six OPTN business members that do not need or have access to the OPTN Computer System. However, it would require that every business organization that requires access to the OPTN Computer System apply for OPTN business membership.

After the business member application is fully complete and the case is prepared for the Membership and Professional Standards Committee (MPSC) Membership Subcommittee, subcommittee member

[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] HRSA FND-2388 – DUA (Data Use Agreement). HHS Contract # HHSH250201900001C.
[8] 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).
[9] HRSA FND-2387 – ISA (Interconnection Security Agreement). HHS Contract # HHSH250201900001C.

reviews are typically completed within two weeks to determine if it is appropriate for the organization to be granted OPTN membership. If the organization is granted interim approval by the MPSC Membership Subcommittee, the member may function as an OPTN member while awaiting review by the entire MPSC and the Board of Directors.[10]

Overall, these requirements would 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, 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.

Revise the Business Membership Bylaw

The Committee proposes revising the requirements for OPTN business membership in order to reduce potential barriers for new and small businesses to become OPTN members. The Committee proposes 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. If the business required OPTN Computer System access in order to fulfill their business functions without this bylaw change, there would be no avenue for new businesses to gain membership. In addition, the Committee proposes 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 is proposing that an alternate representative be required for business members. Currently, transplant hospitals, OPOs, and histocompatibility labs all require a primary and an alternate representative for their organization 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 isn't a single point of failure.

While meeting the security requirements that are outlined later in this proposal may be a potential barrier to OPTN Computer System access for smaller businesses, the Committee feels that the security requirements are a necessary safeguard for candidates, donors, recipients, and their Protected Health Information (PHI).

Business Member Users within the OPTN Computer System

All businesses are reviewed prior to access credentialing. This review includes confirming that the reasons for access are permissible and meet current OPTN policy requirements, and ensuring the list of users is permissible. The business must have an active contract with an OPTN member.

Additional reviews are conducted throughout the year to ensure access is still needed and the business still meets all requirements. Businesses are expected to respond within the determined time frame to

[10] OPTN *Bylaws A.1.C: MPSC Review of the Completed Membership Application*.

complete the business review. If businesses do not respond within the allotted time frame, access to the system could be removed.

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 transplant hospital, OPO, and histocompatibility lab access were not clearly specified in policy, and authorized purposes for business member access were interpreted more broadly.

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

The Committee is also proposing 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.[11] 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. [12]

This proposal prohibits any organization to access the OPTN Computer System for research purposes. 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."[13] This means that the OPTN does not have the authority to provide such identified data without ensuring that researchers have appropriate protections in place. The OPTN Computer System provides data, supplied by member institutions, to authorized users to provide necessary information for patient care, which is more information than should be available to researchers without additional security controls. 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 Computer System is not the appropriate vehicle for the provision of this data.[14] Often, data supplied by an OPTN member is combined with data about donors or patients supplied by other members, and therefore includes more data than would be appropriate for minimum necessary disclosure.

[11] 45 CFR §164.501.
[12] 45 CFR §164.506(c)(4).
[13] 42 CFR §121.11(b)(1)(v).
[14] 42 CFR §121.11(b)(1)(vii).

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.[15,16] 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".[17] 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 to be submitted for HRSA approval. Requests for de-identified limited data sets or aggregated data, either standard or custom, follow a similar data request process.

This proposal will remove the ability for any organization to access the OPTN Computer System for research purposes or to place organs for purposes other than transplantation. The OPTN Computer System is intended to be used "to match organs and individuals included in the [waiting] list,"[18] and the OPTN Computer Match Program specifically "means a set of computer-based instructions which compares data on a cadaveric organ donor with data on transplant candidates on the waiting list and ranks the candidates according to OPTN policies to determine the priority for allocating the donor organ(s)."[19] Access to OPTN data for purposes other than matching is authorized under the OPTN Final Rule, OPTN Contract, and OPTN System of Records Notice (SORN), but such access is not provided or controlled through the OPTN Computer System.[20,21,22] The OPTN System of Record Notice (SORN) requires that if a record is disclosed for research purposes, in each case the data recipient must:[23]

> "(1) establish strict limitations concerning the receipt and use of patient-identified or center-identified data;
> (2) establish reasonable administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or disclosure of the record;
> (3) remove, destroy, or return the information that identifies the individual or center at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the research project, unless the data recipient has presented adequate justification of a research or health nature for retaining such information; and
> (4) make no further use or disclosure of the record except as authorized by HRSA or its contractor(s) or when required by law;"

Therefore, access to OPTN data is controlled through other OPTN processes, with oversight from HRSA.

Any organization that previously used the OPTN Computer System to place organs for purposes other than transplantation will still be able to submit data requests via the OPTN data request pathway, or work with OPOs to access the OPO's electronic medical record (EMR) directly for donor data to place organs for purposes other than transplantation. These organizations would also be able to apply for OPTN business membership if they chose to do so.

---

[15] 45 CFR §164.512 (i).
[16] 42 CFR §121.11(b)(1)(v).
[17] 42 CFR §121.11(b)(1)(v).
[18] 42 USC §274(b)(2)(A)(ii).
[19] 42 CFR §121.2.
[20] 42 CFR §121.11(b).
[21] OPTN Contract HHSH250201900001C, Task 3.7: Access to official OPTN data.
[22] System of Record Notice 09-15-0055, https://www.federalregister.gov/documents/2022/08/01/2022-16344/privacy-act-of-1974-system-of-records. 87 FR 46967 (August 1, 2022).
[23] System of Record Notice 09-15-0055, https://www.federalregister.gov/documents/2022/08/01/2022-16344/privacy-act-of-1974-system-of-records. 87 FR 46967 (August 1, 2022).

Reporting Privacy Incidents

The current policies in place around security incident management require 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 member's computing environment used to access the OPTN Computer System.

This proposal adds additional requirements for privacy incidents involving data obtained from the OPTN Computer System to be reported to the OPTN. This does not mean that any privacy incident involving a member's data on a transplant candidate would need reporting. But, 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 on the member's systems (such as on the member's EMRs), the member must report the incident to the OPTN. 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 a data report from the OPTN Computer System that was involved in a privacy incident.

Data within the OPTN Computer System is provided through the OPTN Computer System by OPOs, histocompatibility laboratories, transplant hospitals, and health care providers, which obtain the information directly from patients or their representatives. Often, records in the OPTN Computer System are supplemented with information from other data sources, such as the Centers for Medicare and Medicaid Services (CMS) and other organizations.[24] While that data may have been assembled, stored, or transformed from data originally supplied by an OPTN member, the data within the OPTN Computer System is OPTN data. As such, the OPTN must ensure the data are properly accessed, secured, and used.

Data Use Agreements (DUAs)

A DUA is an "executed agreement between a data provider and a data recipient that specifies the terms under which the data can be used".[25] 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. To help develop this proposal, the Committee is requesting community feedback on necessary DUA 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."[26] Currently, the OPTN provides Application Programming Interfaces (APIs) as the only method for interconnection to the OPTN Computer System for data exchange. In 2023, over 200 member applications connected to the OPTN computer system via API, and this number continues to rise. All of these organizations will be required to execute an ISA with the OPTN in order to maintain

[24] System of Record Notice 09-15-0055, https://www.federalregister.gov/documents/2022/08/01/2022-16344/privacy-act-of-1974-system-of-records. 87 FR 46967 (August 1, 2022).
[25] 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).
[26] 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).

API connections to the OPTN Computer System, and future connections will require an executed ISA prior to being activated.[27] Organizations that do not integrate with the OPTN Computer System via API will not be required to execute an ISA with the OPTN. Organizations will only be required to execute one ISA per connected member system, regardless of the number of API functions that connection uses or OPTN institutions served via that connection. Therefore, if the member only connects via a single Electronic Medical Record (EMR) at their organization, only a single ISA would be required, even if that EMR serves multiple OPTN members.

[28] 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.[29] 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.[30]

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)".[31] 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.[32] 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 information 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 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 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.

[27] See Appendix A: Sample Interconnection Security Agreement (ISA) Template and Language.
[28] 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).
[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] HRSA FND-2387 – ISA (Interconnection Security Agreement). HHS Contract # HHSH250201900001C.
[31] 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).
[32] 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).

ISAs will be required to be renewed every three years, which is the maximum timeframe allowed by NIST SP 800-53 Rev. 5 guidance.[33] CMS currently requires annual review of their ISAs.[34] 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.

The draft ISA template is available in Appendix A and was developed by the Committee based on the existing Department of Health and Human Services (HHS) ISA template.[35] The Committee is requesting feedback on the draft ISA template as a part of this proposal.

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.

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 security requirements in this section of the proposal, 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.

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.

[33] 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).
[34] 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.
[35] U. S. Department of Health and Human Services (HHS) Office of the Secretary (OS) *Assessment and Authorization (A&A) System Security Plan - Appendix C: Interconnection Security Agreement* (Accessed October 2023).
[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* as of June 27, 2024.
[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).

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'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. Since the implementation of the requirement in August 2023 for transplant hospitals, OPOs, and histocompatibility labs, there have been no information security RFIs sent to members.

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." 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. This incident response plan must include the following:

- Notification of declared security incidents to the Information Security Contact from the member's information security staff
- Notification to the OPTN of declared security incidents occurring on any device that connects to the OPTN Computer System or by which the member provides information to the OPTN as soon as possible, but within 24 hours of the Information Security Contact becoming aware of the declared incident, if the affected users or impacted systems are not disconnected from the OPTN Computer System
- Provision of updates of the remediation status on the agreed upon schedule until the OPTN deems no longer necessary
- Process for acquiring third party validation of proper containment, eradication, and successful recovery, upon request by the OPTN
- Provision of final incident report

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 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 OPTN 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 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.

The Committee understands that security incidents can happen even if the member follows all security controls, and that it is not possible to completely remove risk. Information provided in incident response is used to help members maintain critical transplantation-related functions and to ensure security of the OPTN Computer System.

The OPTN has existing security incident notification requirements, which will not be impacted by this proposal. The OPTN is required to notify HRSA within one hour of a declared security incident, and to follow HRSA's direction regarding any additional notifications.[39]

Transition Procedures

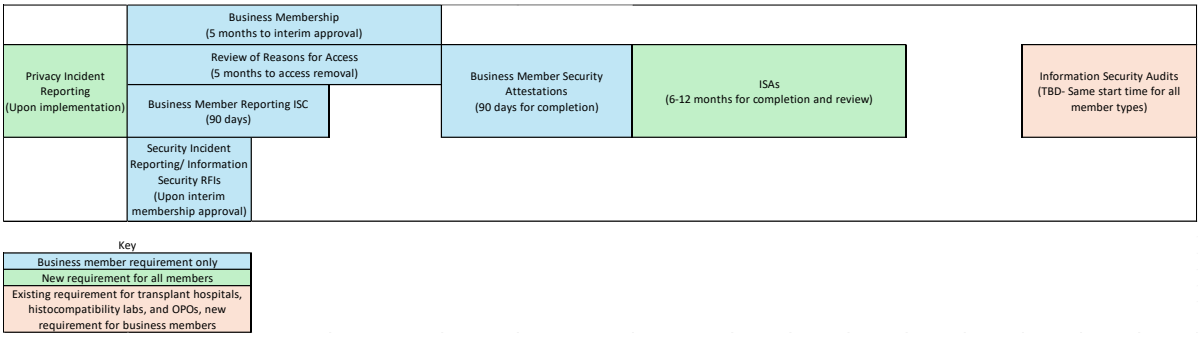
The Committee recognizes that many portions of this proposal require a transition period for members, with some portions of the proposal being dependent on previous portions being implemented. The Committee is proposing an approximately 18-month transition period to fully implement all portions of this proposal, apart from member security audits. Member security audits will be implemented at the

[39] OPTN Contract, HHSH250201900001C, Performance Work Statement (PWS) Task *3.20.4: Incident Response*.

same time for all member types.[40] Reporting of privacy incidents involving data obtained from the OPTN Computer System will be required for all member types after approval of this proposal.

Figure 1 outlines the overall transition period steps, with vertical alignment for steps that are occurring simultaneously. These steps are outlined in greater detail in the following sections.

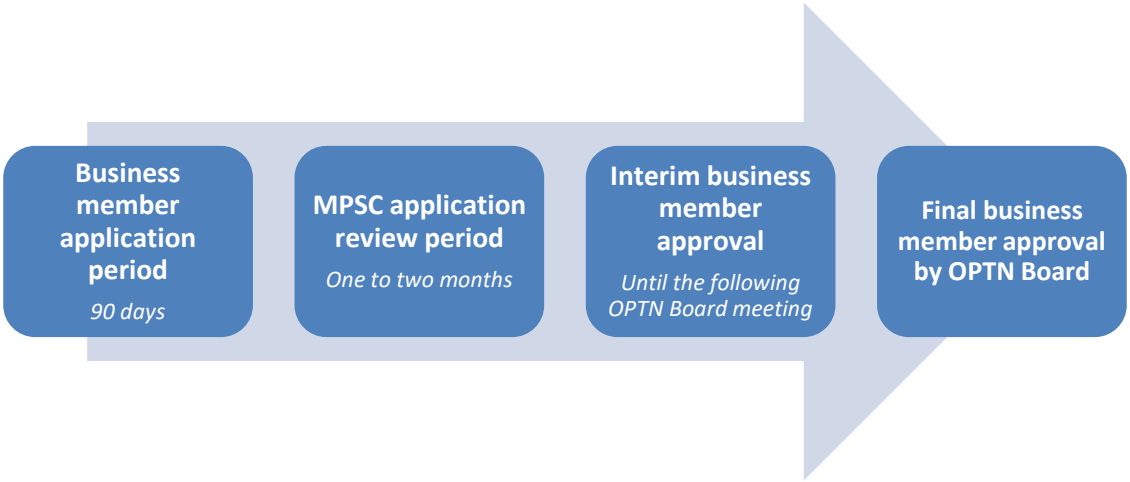
Figure 1: Overall Transition Period Steps



Business Membership

As of May 2024, 27 business organizations who access the OPTN Computer System are not yet business members in the OPTN. Business organizations who access the OPTN Computer System will be provided a 90-day timeframe to apply for OPTN business membership if they are not already members. This 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 *Bylaw 1.7: Business Members*. After interim approval, the member may function as an OPTN member while awaiting review by the Board.[41] The proposed transition period is outlined within **Figure 2**.

Figure 2: Business Membership Transition Period



[40] 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. The Committee is still evaluating the implementation date for this requirement based on review of member security attestations.

[41] OPTN *Bylaw A.1.C: MPSC Review of the Completed Membership Application* as of June 27, 2024.

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.

As of June 2024, 29 percent of business organizations who access the OPTN Computer System are already business members in the OPTN. As of June 2024, there are six business members of the OPTN who do not access the OPTN Computer System. They will not need to reapply for membership in the OPTN.

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

During 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 or manage 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 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

Once the review period for business member attestations is partially complete, the OPTN will send ISA templates to information security contacts at all OPTN members that connect to the OPTN Computer System via API.

NOTA and Final Rule Analysis

This proposal is provided under the authority of the National Organ Transplant Act of 1984 (NOTA) and the OPTN Final Rule. NOTA requires the Organ Procurement and Transplantation Network (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…,"[42] and the OPTN Final Rule, which requires the OPTN to develop "Policies on such other matters as the Secretary directs."[43] To ensure adherence to NIST requirements, the Secretary has directed the development of OPTN policies to require DUAs with every organization that accesses the OPTN Computer System, and ISAs with every organization that interconnects with the OPTN Computer System.

Implementation Considerations

Member and OPTN Operations

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 ISAs 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.

Operations affecting Business Members

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. 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.

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 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.[44] 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

[42] 42 USC §274(b)(2)(A)(ii).
[43] 42 CFR §121.4(a)(6).
[44] 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).

Decision (RBD) with the OPTN Contractor's information security staff. This would require regular updates to the OPTN, 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.

Operations affecting Histocompatibility Laboratories

All members will now be required to report privacy incidents of 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 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.

Operations affecting Organ Procurement Organizations

All members will now be required to report privacy incidents of 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 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.

Operations affecting Transplant Hospitals

All members will now be required to report privacy incidents of 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 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.

Operations affecting the OPTN

The transition plan for this proposal includes review and approval work for 20 business member applications.[45]

The ongoing work for this proposal will require additional information security personnel to review 29 business member attestations a year and perform 29 business member audits every three years.[46] It will require additional information security and information technology personnel to review ISAs of OPTN

[45] Based on OPTN data as of June 26, 2024.
[46] Based on OPTN data as of June 26, 2024.

members who utilize APIs for the OPTN Computer System every three years, and with any interim updates needed.

Projected 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. They rated this project 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.

This project is not anticipated to have a significant fiscal impact on organ procurement organizations, histocompatibility laboratories, or transplant hospitals, however, the 12-hour user removal requirement could impact staffing requirements and require overtime. The FIG cannot make an assessment of the potential fiscal impact on business members though it was identified that the costs to business members could also be distributed across clients such as transplant hospitals or organ procurement organizations and as such would reflect an overall increase in ongoing costs of operations.

Projected Impact on Histocompatibility Laboratories

This proposal is not anticipated to have a fiscal impact on histocompatibility laboratories. The requirement for removal of a user from the system no later than 12 hours after the users last day of employment could pose a burden on staff to maintain, especially over weekends or holidays.

Projected Impact on Organ Procurement Organizations

This proposal is not anticipated to have a fiscal impact on OPOs. The requirement for removal of a user from the system no later than 12 hours after the users last day of employment could pose a burden on staff to maintain, especially over weekends or holidays.

Projected Impact on Transplant Hospitals

This proposal is not anticipated to have a fiscal impact on transplant hospitals. The requirement for removal of a user from the system no later than 12 hours after the users last day of employment could pose a burden on staff to maintain, especially over weekends or holidays.

Projected Impact on the OPTN

It is estimated that 225 hours ($14,554) would be needed to implement this proposal. Implementation would involve updates to the Evaluation Plan, reviewing and preparing implementation communications and educational materials, updates to educational materials, and answering member questions. In addition, implementation would include routine updates to the NOOC through the implementation period. It is estimated that 9,541 hours ($1,696,549) will be needed for ongoing support. For the first-year post-implementation, it is estimated 6,240 hours ($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 3,120 hours ($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 further policy development.

Post-implementation Monitoring

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 renew their ISAs every three years, 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 develop an ISA with 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

Considerations for the Community

- Do you agree with the bylaw changes for OPTN membership regarding small and new businesses?
- Is the proposed transition plan feasible for members?
- Are there any additional obstacles to completing the transition plan that members are aware of?
- A DUA is an "executed agreement between a data provider and a data recipient that specifies the terms under which the data can be used". 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. To help develop this proposal, the Committee is requesting community feedback on necessary DUA requirements.

Policy Language

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 *Bylaws Appendix M: Definitions*. 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 *Bylaws 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, 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 *Bylaws Appendix M: Definitions*.
2. The business member users are granted access to the OPTN Computer System according to *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 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 12 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 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 12 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:

- Appointment of an information security contact, as detailed in OPTN *Policy 3.1.C.i: Information Security Contact*
- Notification to the OPTN Contractor of security incidents occurring in any environment outlined in *Policy 3.1.~~A~~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 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:

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*

Bylaws Language

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.

Bylaw 1.7: Business Members

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.

Appendix A: Sample Interconnection Security Agreement (ISA) Template and Language

This draft ISA is provided for illustrative purposes only and is not the final document. This draft ISA provides the public with an idea of the type of information that will be required to be provided to complete the ISA.

SCOPE AND PURPOSE

The United Network for Organ Sharing (UNOS) owns and operates, by contract with the Health Services Resources Administration (HRSA) ("the OPTN Contract"), the Organ Procurement and Transplantation Network (OPTN) Computer System known as UNet^{SM} on behalf of the OPTN. UNOS allows the direct connection of two or more information technology (IT) systems for the purpose of sharing data and other information resources.

It is a requirement of the OPTN that any IT system that exchanges data with the OPTN Computer System through APIs must have a signed interconnection security agreement (ISA) on file with UNOS prior to connecting the system(s) into the production environment. The ISA must be signed by an official with the appropriate level of authority within the organization seeking to connect a system(s) to UNet^{SM} (e.g., Chief Information Security Officer (CISO) or Equivalent, Chief Information Officer (CIO), Chief Executive Officer (CEO) or President, General Counsel)

TECHNICAL AND SECURITY SPECIFICATIONS FOR SYSTEM INTERCONNECTION

This interconnection security agreement between the OPTN and [OPTN Member Institution] pertains to the specified technical and security requirements regarding the interconnection between the OPTN Computer System and [insert name of connecting Member Institution's system].

A signed ISA is required prior to establishing the connection between the two systems.

The standard interaction that can be obtained between the interconnected systems include, but are not limited to:

- The exchange of data and information between systems
- Customized levels of access to proprietary data sets
- Integrity verification of data
- Real time information exchange to facilitate the transplantation process
- Minimization of data entry burden

SYSTEM DESCRIPTION

OPTN Computer System

System Description

The Organ Procurement and Transplantation Network (OPTN) is a private nonprofit entity that has an expertise in organ procurement and transplantation and was created by the National Organ Transplant Act of 1984 (42 USC §274 et seq., "NOTA"). NOTA sets forth the mission of the OPTN, and the Secretary of HHS promulgated regulations for the operations of the OPTN in 2000. 42 C.F.R. Part 121 (the "OPTN Final Rule"). The OPTN promotes long, healthy, and productive lives for persons with organ failure by promoting maximized organ supply, effective and safe care, and equitable organ allocation and access to transplantation; and doing so by balancing competing goals in ways that are transparent, inclusive, and enhance public trust in the national organ donation system.

The primary function of the OPTN is maintaining a national system through the use of technology and in accordance with established medical criteria, to match donated human organs to potential recipients. It is the only system in the country that serves this function for heart, lung, liver, pancreas, intestine, kidney, and vascular composite allograft (VCA) transplants. By contract with the United States Department of Health and Human Services, Health Resources and Services Administration (HRSA), UNOS serves as the OPTN. To ensure that the OPTN meets both its statutory obligations under NOTA and that UNOS meets its contractual obligations to HHS to operate the OPTN Computer System ("a national system, through the use of computers and in accordance with established medical criteria, to match organs and individuals included in the list"), UNOS owns and operates a proprietary system (UNet^{SM}). Different components of this contractor owned, contractor operated system maintain an active list of patients waiting for transplants, provide OPOs with the ability to list organ donors, and facilitate the organ matching function.

Through the OPTN contract, UNOS agreed to collect specified data on OMB approved forms under the Paperwork Reduction Act. As an additional term of the OPTN Contract, UNOS agreed that any personally-identified or personally identifiable data obtained under the OPTN Contract will be maintained according to the OPTN/SRTR/HRSA Data System of Records, HHS/HRSA/HSB/DoT, No. 09- 15-0055, including data maintained electronically, and must be disclosed consistent with the Privacy Act and the Systems Routine Uses, outlined in the applicable System of Records Notice.

System Location

The OPTN computer system is hosted in geographically separated data centers. The East Region (ER) data center is in Sandston, Virginia and the West Region (WR) is located in Irving, Texas. Both datacenters are operated by Quality Technology Services (QTS).

User Community

The primary users of UNet^{SM} are authorized staff at Transplant Hospitals, Organ Procurement Organizations, and Histocompatibility Laboratories.

The UNet[SM] user base consists of UNOS staff, UNet[SM] Site Administrators, and UNet[SM] users.

UNOS staff are granted access to UNet[SM] as needed for their job roles. This access allows them to view information within UNet[SM] for all member institutions as needed for their role. Staff in privileged access roles are also responsible for maintaining the applications and infrastructure.

UNet[SM] Site Administrators are individuals identified at each member organization who are responsible for administering UNet[SM] users for their institution and managing appropriate permissions to view/edit data in the system.

UNet[SM] users are individuals who are granted access by their Site Administrators and only have access to their specific transplant program(s)' data.

Points of Contact

Role	Email	Phone
OPTN Member Risk Management	risk.management@unos.org	
Privacy	privacy@unos.org	

Name of Connected System

System Description

System Location

User Community

Points of Contact

Role	Name	Email	Phone
System Owner			
Information System Security Officer			
OPTN Security Point of Contact(s)			

TOPOLOGY DRAWINGS

Insert one (or more) visual diagrams detailing the interconnected systems and data flow.

DATA DESCRIPTION

Purpose of Data Exchange

Data is exchanged between the OPTN Computer System and [Member Institution's system] for the purpose of data transfer between information systems to facilitate organ transplantation processes.

Description of Data to be Transmitted

[provide a description of the data being transmitted]

Data Sensitivity

OPTN data is categorized as **HIGH** based on FIPS 199 Standards for Security Categorization of Federal Information and Information Systems and the guidance of NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories. This data categorization matches the overall system security categorization found in the OPTN Systems Security and Privacy Plan which is a part of this systems certification and accreditation package.

INFORMATION EXCHANGE SECURITY

THE OPTN and Member Institution will take necessary steps to secure the interconnected systems and information exchanges in accordance with applicable laws and regulations. The OPTN Computer system is secured utilizing the NIST 800-53 Rev5 High Baseline, and interconnected systems are expected to be secured at minimum following the NIST 800-171 Rev2 security framework.

Operational Security Mode

OPTN Computer System = {(Confidentiality, **M**), (Integrity, **H**), (Availability, **M**)} = High

Member Institution's system= {(Confidentiality, **H/M/L**), (Integrity, **H/M/L**), (Availability, **H/M/L**)}

Rules of Behavior

UNet[SM] and [Member Institution's system] users are expected to protect data in accordance with the policies and standards of the OPTN, the OPTN Systems Terms of Use, the OPTN API Terms of use, and each systems' respective Rules of Behavior.

Formal Security Plans

The OPTN Computer System maintains an Authorization to Operate (ATO) from HRSA that is renewed on a recurring basis and dependent on Security Control Assessment results. The following security documents have been developed for the OPTN Computer System:

- System Security and Privacy Plan (SSPP) MM/DD/YYY
- Information Technology Contingency Plan (ITCP) MM/DD/YYY
- Incident Response Plan MM/DD/YYY

Member Institution's System has in place the following Security Plans:

- System Security and Privacy Plan (SSPP) MM/DD/YYY
- Information Technology Contingency Plan (ITCP) MM/DD/YYY
- Incident Response Plan MM/DD/YYY

Risk Management

The Organ Procurement and Transplantation Network (OPTN) reviews its members for compliance with OPTN information security requirements outlined in OPTN *Policy 3.1: Access to the OPTN Computer System* on a periodic and ad hoc basis. The OPTN Contractor, United Network for Organ Sharing (UNOS) manages the policy requirements, and the Network Operations Oversight Committee (NOOC) is delegated to take actions on behalf of the OPTN Board of Directors in oversight of these requirements.

These requirements are evaluated based on annual self-attestations, and recurring audits, submitted to the OPTN on behalf of the member and reviewed by NOOC for actions necessary. Any necessary actions are communicated to the member via their Information Security Contact(s).

Members are expected to take corrective actions to risks identified through the compliance monitoring program. If corrective actions are required, these will be communicated to a member's information security contact(s) from OPTN Contractor Information Security staff.

Incident Reporting and Response

Per OPTN Policy 3.1, OPTN Members are required to name a security point of contact at their institution, and to report incidents as soon as possible, but no later than:

- 24 hours following the information security contact becoming aware of the security incident if a member does not disconnect the affected users and any impacted systems from the OPTN Computer System
- 72 hours following the information security contact becoming aware of the security incident if the member does disconnect the affected users and any impacted systems from the OPTN Computer System

A security incident at the member institution may warrant a review of the member and a request for additional information related to the member's information security. If corrective actions are required, these will be communicated to a member's information security contact(s) from OPTN Contractor Information Security staff.

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 which may extend to a request to disconnect from the OPTN Computer System.

Awareness and Training

The parties agree that all current employees and contractors are required to complete the initial and all annual refresher security awareness training provided by Member Institution. This training provides all new employees with the initial training requirements, including computer usage, information security, physical security access, and incident response initiatives. All users are required to undergo annual refresher training. In addition, Member Institution's system users receive training on updated system components, administration, and security requirements for any newly installed components. Member Institutions must retain training records and make them available upon OPTN's request.

In addition, users of the OPTN computer system are required to complete OPTN Security Awareness training annually.

Auditing

Both organizations are responsible for auditing application processes and user activities involving this interconnection. Activities that will be recorded include: event type, date and time of event, user identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for a minimum of twelve (12) months.

VALIDITY

This ISA is valid for 3 years after the latest date on either signature below if the technology documented herein does not change or if there are no other intervening requirements for update. At that time, it must be reviewed, updated and reauthorized. Noncompliance on the part of the party and/or its employees or contractors with regards to security policies, standards and procedures explained herein may result in immediate termination of this agreement.

TERMINATION PROCESS

Describes the process for terminating the interconnection agreement, including how data and access will be securely decommissioned.

(this section is in development)

AMENDMENT AND MODIFICATION PROCEDURES

Provides procedures for amending or modifying the agreement as needed, including how changes will be communicated and agreed upon by all parties.

(this section is in development)

LIABILITY AND INDEMNIFICATION

Clarifies the liability of each party in case of a breach or security incident, and any indemnification clauses.

(this section is in development)

SIGNATORY AUTHORITY

_____	_____
Full Name, Date	Full Name, Date
OPTN Authorizing Official	Member Institution Authorizing Official