OPTN ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK Meeting Summary

OPTN Network Operations Oversight Committee
Meeting Summary
December 16th, 2022
Webex

Edward Hollinger, MD, PhD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 12/16/2022 to discuss the following agenda items:

1. Welcome
2. OPTN Member Information Security Policy and Bylaw Enhancements

The following is a summary of the committee's discussions.

1. Welcome

Ed Hollinger, Chair of the Network Operations Oversight Committee (NOOC), introduced the main purpose of the meeting was to continue the committees' discussion about the network security project. The goal of the meeting was for the committee to review the proposed language and vote on the proposal to be submitted for Winter 2023 Public Comment.

2. OPTN Member Information Security Policy and Bylaw Enhancements

Rebecca Murdock, Senior Policy Counsel, reintroduced the project and the progress that had been completed last meeting. The committee discussed the entirety of the proposed language that would be sent out for public comment. The changes that were made to the policy language were highlighted for their awareness and the committee was encouraged to discuss and ask any remaining questions they had about the proposed language. Miscellaneous changes were made to the language during the meeting by the committee to ensure that the proposal read as they intended it to.

The proposed language was broken down into the various topics the committee discussed throughout the past few months. They discussed the proposed language by the different areas of focus their discussions were based around. They review the final proposed language for attestations, audits, and member compliance. Definitions were also recapped and edited to ensure they represented what the committee intended.

Summary of Discussion:

At the beginning of the meeting, a committee member asked for clarification about the training portion of the proposal. It states that members will be required to complete testing and training to have access to the OPTN Computer System and they wanted clarification on whether this was currently the practice. Staff confirmed that this is currently a requirement for site administrators, but this will now be a requirement for all users. Another member asked for clarification on the requirement of two employees from each program to act as the site administrator and the site administrator backup. They asked why it was two people for each program as opposed to each member. The committee discussed that if a member had multiple programs than the same two people could be listed multiple times. It was noted that if there are two people validating each other's work and there is a check and balance system to better secure the network.

The proposed language for attestations was discussed in depth on whether the OPTN would be sending members a 'checklist' to use when attesting to the framework requirements. UNOS staff explained that the OPTN would provide values to members and have them self-attest to these values. Their work would later be used as verification during their audit. A representative from HRSA commented that if the language said that attestations would be performed annually then they would not be able to perform them more routinely if necessary. Ms. Murdock explained that the language says the OPTN Contractor may request attestations from members at any time. This means that the language covers the OPTN to request more frequent attestations from members if necessary. When discussing data fields, a representative from HRSA wanted to clarify that this work will not be included in data collection so therefore this is not something that would need OMB approval. A committee member asked when attestations would be due for new members, and wondered whether the OPTN would require an attestation before they were granted access to the OPTN Computer System. UNOS staff explained that one of the operational pieces of the policy could allow for temporary access to act as a grace period for members. The OPTN could then require an attestation be performed within a specified timeframe. A representative from HRSA thought that members should have to self-attest to the security framework requirements before they are granted access to the OPTN Computer System; a committee member agreed that new members must meet the security requirements before receiving access to the system and additionally suggested that attestations were for existing members and ongoing membership.

The committee revisited the conversation around two site security administrators. A UNOS staff member explained that the request for two site security administrators per program as opposed to per member was to try and ensure the data was protected by people close to the programs. Because these administrators would be granting members access to program specific data, this was another measure to protect the data. However, they reiterated the fact that someone can be a site administrator for multiple programs within the member institution.

When discussing security incident management and reporting, a committee member suggested that members should work with the OPTN Contractor when it comes to containment. Ms. Murdock noted that the language covered this by including that the OPTN may require a member perform certain precautionary measures to contain the risk, which could include onsite remediation or disconnection.

A representative from HRSA thought it important to draw a distinction between what the OPTN Contractor is responsible for and what the OPTN is responsible for. UNOS General Counsel, Jason Livingston, agreed that it is important for the NOOC to determine what authority each body has and what the roles and responsibilities of each group has. Mr. Livingston posed the question regarding authority in terms of disconnecting members from the system and asked if the body making the choice to disconnect a member is the same entity that would have the decision-making authority as a whole. The relationship between the OPTN and the OPTN Contractor was not discussed in the policy language. A committee member asked whether the OPTN Contractor has the authority to act on behalf of the OPTN, whether it would be a shared decision, or whether the OPTN could overrule the OPTN Contractor. UNOS staff suggested using a passive voice when incorporating language surrounding authority to ensure that the language can adapt to any future changes between the OPTN and the OPTN Contractor.

A representative from HRSA commented that HRSA and the OPTN have been discussing standard operating procedures during security incidents because they want to ensure that proper procedures are put into place for the future. UNOS staff detailed internal work that has been done at UNOS to create an incident response section of a response plan. The response plan details what actions UNOS would need to take if an event were to occur. The plan allows for a consistent and calculated approach across the organization.

A committee member thought this information could be important for the NOOC to share with the community. They thought that this could help illustrate to members that the process is not to be punitive but is set up to contain any issues in the event of a security incident. They also thought that it was important to show members that the OPTN Contractor is doing the same work across their organization and how important it is.

A representative from HRSA asked if a member's system were compromised and posed a threat to the OPTN Computer System as a whole, would the member be disconnected even if that means that transplants in their organization could decrease. UNOS staff commented that they want to ensure transplants are still taking place even when a security incident occurs. The representative from HRSA explained that they were concerned members could challenge the OPTN shutting down their system and whether this was something they needed to consider. A committee member reiterated their comments from earlier that it is important for members to not view the process as punitive. Members need to view the process as a cooperative opportunity between them and the OPTN to ensure the security of the transplant system.

Next Steps:

The committee discussed next steps for the proposal and what to expect during public comment. Some topics they could expect to discuss deal with member compliance, minimum security values, how to handle policy violations, how to report events, and noncompliance review. The committee chair thought it was important for the NOOC to represent the policy and show the community that the NOOC is more interested in finding out about security holds and mitigating security risks rather than punishing anyone.

Vote:

The committee unanimously approved the proposed policy language, as written, to be sent to the Executive Committee to release for winter 2023 public comment.

Attendance

- **Committee Members and Advisors**
  - Adam Frank
  - Clifford Miles
  - Daniel Yip
  - Ed Hollinger
  - Jeff Sterrette
  - Kelley Hitchman
  - Melissa McQueen
- **HRSA Representatives**
  - Adriane Burton
  - Adrienne Goodrich-Doctor
  - Arjun Naik
  - Chris McLaughlin
  - Cliff Myers
  - Vanessa Arriola
  - Vinay Viyyuru
- **UNOS Staff**
  - Alex Tulchinsky
  - Amy Putnam
  - Anna Messmer
  - Bonnie Felice
  - Bridgette Huff
  - Jason Livingston
  - Jerry DeSanto
  - Kristine Althaus
  - Liz Robbins Callahan
  - Michael Ghaffari
  - Morgan Jupe
  - Rebecca Murdock
  - Rob McTier
  - Susie Sprinson
  - Terri Helfrich
  - Tiwan Nicholson