OPTN ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK Meeting Summary

OPTN Network Operations Oversight Committee
Meeting Summary
December 12th, 2022
Webex

Edward Hollinger, MD, PhD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 12/12/2022 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 purpose of the meeting was to continue to committee's discussion about the network security project. The committee met to discuss proposed changes to the policy and to discuss feedback received from the Executive Committee and the Policy Oversight Committee (POC). The NOOC also recapped their presentation to the Transplant Administrators Committee Fiscal Impact Advisory Workgroup on the anticipated financial impact associated with the project.

Dr. Hollinger recounted his presentation to the Executive Committee and shared the committee's feedback. The Committee was overall supportive of improving the security system but had suggestions on topics the NOOC should concentrate on. The committee suggested consistency in standards across the healthcare industry and transplant systems, they suggested the NOOC consider the variability in scope between different member types and member sizes, they urged the committee to detail their proposed plan to enforce compliance, and they suggested the committee consider the cost impact this could have on members. The Executive Committee focused heavily on enforcement of compliance and encouraged the NOOC to consider the role the MPSC may play.

The Policy Oversight Committee had similar feedback to the Executive Committee and asked questions about the committee's plans on educating members on the changes and how they planned to support less mature members achieve these standards. The POC also asked the NOOC to consider the device members are using and whether the policy covers the monitoring of someone's personal device versus a device owed by the member institution. The NOOC discussed the different levels of access granted to the OPTN Computer System and that this will cover the issue associated with members using their own personal devices to access the network.

2. OPTN Member Information Security Policy and Bylaw Enhancements

Rebecca Murdock, Senior Policy Counsel, introduced the objective of the meeting was to focus on security framework, incident response, and member compliance drafting. Since last meeting, UNOS staff incorporated feedback from the committee on the framework to include that member compliance is held to a NIST standard or a NIST equivalent standard security framework. The proposed language also stated that the OPTN will maintain a list of minimum security control values based on the security framework that OPTN members must adopt. This was incorporated due to feedback received from the NOOC that it would be helpful for members to have a list of steps to checkoff when ensuring their system is up to standard.

When discussing incident response, Ms. Murdock asked the committee to consider who the contact should be between the member institution and the OPTN during a security incident and the role the contact would play. The language suggests that each OPTN member with access to the OPTN Computer System should identify an information security contact and comply with a written protocol for the information security contact to fulfil the responsibilities detailed in the policy. The committee also discussed the timeframe members had to report an incident to the OPTN. The drafted policy language stated that members should report the incident as soon as possible but must report no later than 24 hours after becoming aware of the incident. The committee discussed whether 24 hours was an appropriate timeframe for the OPTN and suggested posing this question to the community during public comment. The committee also discussed suspension of access when it comes to incident response and if the OPTN should develop criteria for suspending OPTN member organizations and OPTN member user accounts. It is a requirement of the contract modification from HRSA to develop criteria for suspending access. The committee agreed it was important that the terms of suspension were detailed in the policy for members to be aware of.

The committee discussed establishing a process for monitoring member compliance with the OPTN member security framework. Compliance was divided into three parts: attestations, audits, and monitoring. The committee discussed requiring an annual self-attestation from members to ensure they are adhering to the framework. The draft language included a required annual attestation from members but also stated that the OPTN could request more frequent attestations from members when necessary. When discussing compliance, the committee noted it was important to view compliance violations in two different categories. The first was a security incident with potential noncompliance and the other was when no security incident had occurred but there was also potential noncompliance to the framework. The committee detailed what course of action could be taken following a compliance review to members and the severity of the actions.

Summary of Discussion:

When discussing the security framework requirements, a committee member thought it was important to highlight that some members may have a difficult time with all the acronyms and technical language. They suggested the OPTN include supporting documents on what the acronyms were. They thought this may help members feel more comfortable and less intimidated by the language. The committee discussed the importance of ensuring the process is detailed in plain language, so the community understand what is being proposed. A representative from HRSA thought it was important for the OPTN to refer members to the NIST website for official definitions. Committee members and advisors agreed that it was beneficial to use existing definitions and to refer members to these sources.

When discussing incident response and an information security contact, a committee member asked if there were any ideas to include a backup contact for best practices. UNOS staff and committee members thought it was important for member institutions to have more than one contact but was not necessary to include in policy. A committee member asked if the contact would be someone within the transplant field or whether it would be someone from their institutions IT department. They suggested the OPTN describe how this has worked in the past for members to follow best practices when designating their contacts.

When discussing the timeliness of reporting, the committee discussed whether 24 hours was an appropriate amount of time to report an incident. The committee thought that the language of "as soon as possible but no later than 24 hours" was appropriate but thought that clarification was necessary on whether this pertained to security events, security incidents, or both. A committee member raised the concern of whether personal cellphones would be included when it came to security incidents. For example, they asked if someone lost their personal phone where they access to the OPTN Computer System, is this something that should be reported to the OPTN or are there different levels of security incidents. A committee member asked if it would be beneficial for the committee to detail the different threat levels associated with different ways people access the OPTN Computer System.

When discussing draft policy language about the suspension of access to the OPTN Computer System, a committee member thought it would be beneficial to include the alternative ways members can access the OPTN Computer System if their access is cut off due to a security incident. They thought it was important to include in the policy that transplants will not be affected if access is suspended. They discussed whether or not this was something that should be included in the policy language.

When discussing member compliance to the security framework, a committee member thought it was important that good faith efforts to comply with the framework would not be sent to MPSC for review. They worried that if these incidents were sent to the MPSC then members may hesitate to report security incidents. Other committee members agreed that the goal is for members to self-report and to keep the system secure and would not want to inadvertently disrupt that by failing to deviate between the two compliance issues. Committee members agreed that there cannot be ramifications that discourage members from reporting. They suggested that the OPTN act a resource for members to grow their frameworks and to educate them on ways to better secure their network. A representative from HRSA noted that the MPSC may not be the correct body to handle these incidents and suggested the committee modify Appendix L to note that the NOOC will work with the MPSC to respond to incidents.

Next Steps:

The committee will meet again on Friday, December 16th to discuss these proposed changes to the policy language. The committee plans to vote on the proposal on Friday to submit for Winter 2023 Public Comment.

Upcoming Meetings:

- December 16th

Attendance

- **Committee Members and Advisors**
    - Adam Frank
    - Bruno Mastroianni
    - Clifford Miles
    - Daniel Yip
    - Edward Hollinger
    - James Pittman
    - Kelley Hitchman
    - Melissa McQueen
- **HRSA Representatives**
    - Adriana Martinez
    - Adrienne Goodrich-Doctor
    - Chris McLaughlin
    - Cliff Myers
    - Demonique (Nick) Lewis
    - Satish Gorrela
    - Vanessa Arriola
    - Vinay Vuyyuru
- **UNOS Staff**
    - Alex Tulchinsky
    - Amy Putnam
    - Bonnie Felice
    - Bridgette Huff
    - Janis Rosenberg
    - Jason Livingston
    - Kristine Althaus
    - Liz Robbins Callahan
    - Marty Crenlon
    - Michael Ghaffari
    - Morgan Jupe
    - Rebecca Murdock
    - Rob McTier
    - Roger Brown
    - Susie Sprinson
    - Terri Helfrich
    - Tiwan Nicholson