OPTN Network Operations Oversight Committee
Meeting Summary
May 8th, 2023
Webex

Edward Hollinger, MD, PhD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 05/08/2023 to discuss the following agenda items:

1. Welcome
2. Closed Session
3. OPTN Member Information Security Policy Enhancements

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

1. Welcome

Dr. Ed Hollinger, Chair of the Network Operations Oversight Committee (NOOC), welcomed committee members and provided an overview of the agenda.

2. Closed Session

The committee met in a closed session.

3. OPTN Member Information Security Policy Enhancements

Ms. Courtney Jett, Policy Analyst, recapped the policy language changes that were made during the April 13 meeting. These changes included changing "compliance with" to "adherence to" as it related to a security framework, removing the requirement for OPTN minimum control values, clarifying that only portions of a member's incident response plan involving access to the OPTN Computer System must be available upon request, narrowing the scope of information security framework, and revising the timeline for reporting information security incidents. Ms. Jett also shared what language changes have been made as it relates to scope.

Ms. Jett reviewed the proposed timing on security incident reporting, which is currently 72 hours following the knowledge of a security incident taking place. Ms. Jett stated that steps members should take are not explicitly included in the policy language, but just creates the threshold of whether or not a member user is disconnected from the OPTN Computer System.

The committee discussed removal of access to the system, including what the MPSC expedited review process is, additional protective actions the OPTN Contractor may take prior to removal of access, analysis of the legal ability of removing access as the OPTN Contractor, and the policy language. Ms. Krissy Laurie, Senior Implementation and Evaluation Analyst, presented on the expedited MPSC review process. Ms. Laurie explained that the MPSC is routinely asked to provide an expedited review and determination for member cases which include patient safety concerns and program/key personnel interim approval. She explained that the review process is usually conducted through MPSC subcommittee review. Alternatively, the MPSC leadership group which may be called for emergency review, and this review primarily is conducted by the Chair or Vice Chair of the Committee.

Ms. Jett presented non-routine protective actions prior to removal of access for members. These actions could include the suspension of individual user access for violation of terms of service such as an attempt to harm the OPTN Computer System as well as unauthorized use of sharing of OPTN data. Other actions could include member suspension of API access, requesting members voluntarily disconnect from the OPTN Computer System, removing file upload abilities while still allowing manual data entry, blocking IP addresses that are indicators of compromise, and other actions as appropriate and necessary based on the type of incident.

Mr. Jason Livingston, General Counsel, presented on the legal analysis on the OPTN contractor's ability to remove access without HRSA or the NOOC directing the contractor. Mr. Livingston explained that the OPTN Contractor does not have that authority by means of any written policy or in the OPTN Contract.

The committee reviewed the language associated with removing a member's access and the changes that the committee had suggested during prior meetings. The committee ultimately decided to use language that stated that 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 language also stated that any action 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.

Ms. Jett summarized the policy language changes that were made during the call to the committee. These language changes were found in the incident response plan that the committee discussed and agreed to on the call, and the language disconnecting users or impacted systems from the OPTN Computer System. Committee members were shown the language and were able to review the flow of the changes with the already existing language.

Towards the end of the meeting, the committee had robust conversation around policy language and educational requirements. The committee also discussed how operational discussions would be a next step in the committee's work.

Summary of discussion:

When discussing the language around scope, a representative from HRSA questioned the inclusion of the word "interface" and whether this was the appropriate word as it relates to third-party users. Ms. Jett explained that access for third-party users is in a different section of the policy language and that they must adhere to an approved framework.

A committee member asked about security incident reporting and suggested that when the policy says that impacted users will be disconnected, that it will be impacted systems not necessarily users. They were concerned over this wording and thought that the difference was impactful. There was discussion amongst the committee members about what the impact could be from a user or a system, so to specifically note one of them would not be useful. Ms. Jett suggested including "impacted user and/or system" to the policy language, to which committee members, and representatives from HRSA agreed was an appropriate measure. A representative from HRSA asked if there was a requirement to disconnect a user, independent of the reporting. Ms. Jett responded that the policy language states that users may be directed to take other actions, but it is not specified that they must be disconnected in a specific timeframe, just that they report in an appropriate timeframe. Ms. Jett shared some of the other actions that users could be directed to take by the OPTN, as stated in OPTN Policy. A committee member asked about the policy language in time to report an incident, as it states that members have 24 hours from learning about the incident to report it to the OPTN, they wondered if this is from when an incident occurs or from when an event is declared to be an incident. Ms. Jett explained that with the committee defining a security incident as an event that is declared as jeopardizing, then this means that it would be 24 hours after the information security contact becomes aware of the security incident. Ms.

Jett also suggested that the committee could provide educational materials to members to ensure this is clear to them.

When discussing the MPSC expedited review process, a representative from HRSA stated that they did not foresee the NOOC asking centers to inactivate. They asked that if a member is not permitted direct IT connection to the OPTN Computer System, would the Organ Center be able to offer alternative ways for the member to engage with the OPTN to place organs and accept offers. The representative saw this as a way to avoid inactivating a program but to instead have them operate outside of directly connecting to the OPTN Computer System. Ms. Jett agreed that the NOOC would not be asking members to inactivate but would most likely be asking members to disconnect from the OPTN Computer System. A committee member suggested that the NOOC consider, on behalf of the OPTN, making some changes around data submission on data that is not required for immediate transplant functions.

When discussing non-routine protective actions prior to removing access, a committee advisor suggested that, in the future, the committee consider the different member types when discussing removal of access. They stated that different member types have different capabilities when it comes to reacting to a security incident, and members have different risks associated with each. A committee member thought that this could rely on the subject matter experts at member organizations to discuss their next steps and talk to the OPTN about their analysis of the situation. The subject matter experts at each member hospital also know how to help their member continue on with their life saving work, while also considering the integrity of the OPTN Computer System.

A representative from HRSA, when discussing the legal analysis, noted that HRSA would need in writing that the OPTN Contractor does not have the authority to do this and is not something within their means to provide. The representative commented that the Organ Center should be able to provide support to these organizations should they need it. Ms. Jett responded that the Organ Center is currently staffed for their day-to-day operations and if they had to undertake assisting multiple members, it would be a huge undertaking. The representative from HRSA responded that this is not a staffing issue but is a contract issue or budget issue. They stated that the OPTN Contract requires that Organ Center assist members when necessary and that the OPTN needs to provide an alternative to members for assistance if their system is compromised. Ms. Rebecca Murdock, Senior Policy Counsel, explained that the assistance members would need if their system was compromised would look different for the different member types. She explained that the Organ Center does have similar capabilities as an OPO but not that of a transplant center or histocompatibility labs. Mr. Livingston commented that asking this of the contractor would be an incredible responsibility, without direction from the government or the OPTN. A committee member commented that they think it is important to rely on the leadership of the NOOC when it comes to taking action on behalf of the OPTN. They commented the importance of making sure that the transplant system at large is protected, even if that means having to suspend the access of a member; having a process in place will help to mitigate the immediate risk to the OPTN Computer System.

When discussing the policy language on removal of access, a committee member commented that it is important to have a procedure in place for the OPTN and the OPTN Contractor to react to situations quickly and effectively.

While reviewing the policy language changes that were made during the call, a representative from HRSA asked about the use of “and/or” when it came to disconnecting users or affected systems. Ms. Murdock, as the drafter of the policy language, explained that the language throughout the OPTN, and is inclusive of or, so “or” is not necessary to include in the policy language itself. Ms. Murdock explained that she would make sure that it is clear in the resources, implementation, and the briefing paper that members utilize.

A representative from HRSA asked what happens when a member of an impacted system chooses to only disconnect from the impacted system and doesn't mitigate the risk to the OPTN. They asked how the OPTN enforces other users to report incidents to the OPTN within the allotted timeframe. Ms. Jett explained that within the definition of a security incident, the OPTN is able to declare a security incident if there are indications of an incident from a member. The OPTN is permitted to contact members during this time to assess any suspected incidents.

Vote:

The committee voted on the final policy language to Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements. The final proposal will be considered by the Board of Directors in June 2023.

Attendance

- **Committee Members and Advisors**
  - Adam Frank
  - Bruno Mastroianni
  - Clifford Miles
  - Daniel Yip
  - Ed Hollinger
  - Kelley Hitchman
  - James Pittman
  - Melissa McQueen
  - Paul Connelly
- **HRSA Representatives**
  - Adriana Martinez
  - Adriane Burton
  - Arjun Naik
  - Chris McLaughlin
  - Cliff Myers
  - Manjot Singh
  - Nick Lewis
  - Vinay Vuyyuru
- **UNOS Staff**
  - Alex Tulchinsky
  - Anna Messmer
  - Amy Putnam
  - Bonnie Felice
  - Brian Tannenbaum
  - Courtney Jett
  - Jason Livingston
  - Julie Nolan
  - Krissy Laurie
  - Kristine Althaus
  - Liz Robbins Callahan
  - Lloyd Board
  - Melissa DiGiorgio
  - Morgan Jupe
  - Rebecca Murdock
  - Rob McTier
  - Roger Vacovsky
  - Sarah Payamps
  - Susie Sprinson
  - Terri Helfrich
  - Tiwan Nicholson
  - Tynisha Smith
- **Other Attendees**
  - Nathan Kottkamp