OPTN ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK

Meeting Summary

OPTN Network Operations Oversight Committee
Meeting Summary
June 5th, 2023
Webex

Edward Hollinger, MD, PhD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 06/05/2023 to discuss the following agenda items:

1. Welcome
2. Closed Session
3. Network Operations Metrics and Monitoring Report Preview
4. Security Project
    a. Accenture Deliverables
    b. Cybersecurity Incident Planning: Operational Guidelines

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

1. Welcome

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. Network Operations Metrics and Monitoring Report Preview

Mr. Rob McTier, Business Architect, reviewed the Network Operations Metrics and Monitoring Report that spans the reporting period from April 2022 to March 2023. This report, along with the NOOC Chair Report to the Board are an OPTN contract deliverable. The report has six metrics categories: efficiency, availability, accuracy, timeliness, usability, and security. During his presentation, Mr. McTier asked the committee to consider how these metrics could be improved, whether there are new metrics to be developed, and what these metrics tell us about the OPTN Computer System. The Chair of the NOOC also asked the committee to consider whether there were any additional metrics they would like to include in the Chair's Report at the June Board Meeting.

The first efficiency metric is the match run time, which is the first step an OPO takes in the organ allocation process. The total run time is the number of seconds that the algorithm takes to produce a list of potential recipients. The median match run time for kidney is 21 seconds or less, and the median match run time for other organs is under 6 seconds. Since kidney registrations make up over 80% of the waiting list, the kidney match run times tend to be greater than other organs.

After the match run is complete, OPOs use the OPTN Donor Data and Matching System to electronically notify transplant centers of organ offers. Organ offer notification delivery metrics reflect the number of minutes before the OPTN Computer System receives confirmation that a voice notification was delivered. The median organ offer delivery time was slightly more than two minutes throughout the reporting period. The Chair asked for more context on the maximums that were noted and how much of an impact they had, how many users were involved, and whether we understand why these situations occurred. Mr. McTier explained that there was one event that exceeded ten minutes, and after further investigation it was found that a second notification was not needed because the member responded to the email, not the voice notification. Because the member logged into the OPTN Computer System, this stopped the system from sending out a second notification. The Chair asked about the scope of notification. Mr. McTier explained that the graph showed one notification to a transplant center for a set of candidates. He explained that the graph showed notification to just one program, and this did not have to do with notifications to multiple centers about one organ. Mr. Tiwan Nicholson, Senior Director of IT Operations, explained that it is rare for these long response times to occur and there are other channels to communicate with members about organ offers. Mr. Michael Ghaffari, Senior Director of Technology Development, explained that if the OPTN does not hear back from a member within ten minutes, then another communication is sent out. He explained that just because it could take this long to receive confirmation from members, this does not mean that the OPTN Contractor is waiting this long to take other actions.

Mr. McTier then presented on the efficiency metric that deals with the seamless data exchange between APIs. The example presented to the committee showed the percentage of official OPTN Data in the OPTN Waiting List, the OPTN Donor Data and Matching System, and the OPTN Data System that can be submitted as API; the example showed information that could be submitted, but not what was necessarily submitted. Overall, 64% of official OPTN data elements may be submitted through APIs. A committee member commented that the histocompatibility lab OPTN Data System reporting forms are difficult to use. Mr. McTier said that the report would be revised based on this feedback. A committee member asked if there were any ongoing efforts to build an API for histocompatibility lab reporting. Mr. McTier explained that there have been APIs developed for the submission of HLA and unacceptable antigens on the OPTN Waiting List and there is work under way to report donor HLA in the OPTN Donor Data and Matching System. Mr. Marty Crenlon, Healthcare Integration Program Manager, stated that there are no active plans around histocompatibility data for the OPTN Data System specifically, but they are looking at APIs for deceased donor and potential candidate reporting on the OPTN Waiting List and the OPTN Donor Data and Matching System. A representative from HRSA clarified that the information shown was the percentage of data elements that could potentially be submitted through APIs and not the actual percentage that are submitted through APIs. Mr. McTier confirmed that later in the presentation, there would be information on adoption metrics and the percentage of members that do submit data via APIs.

During the reporting period, an API was implemented that would allow for the submission of data that is needed to calculate the lung CAS that was implemented with Lung Continuous Distribution. API projects that are currently in progress include OMB submission that will be implemented in September, there is a new API that would allow for the creation of a deceased donor record for use of OPOs and electronic donor systems, and a new API that would allow for the submission of deceased donor HLA in the OPTN Donor Data and Matching System. A representative from HRSA asked if the list of projects is given to the OPTN Contractor on the work that the NOOC would like to see done. Mr. Crenlon explained that the information is a backlog of work in coordination with members and vendors. The NOOC is encouraged to provide feedback on the upcoming work on API adoption.

Mr. McTier shared information about the percentage of members that are utilizing APIs available to them. The greatest adoption is seen around deceased donor APIs, which allows OPOs to update donor information in the OPTN Donor Data and Matching System during the organ allocation process. 66.1% of OPOs used this API in March 2023. The unacceptable antigen API saw the greatest increase in adoption which saw an increase from 9.1% to 37.3%. There was also an increase in adoption from 10.3% to 44% for APIs that allow users to retrieve information about the OPTN Waiting List registration. This increase was likely due to the decommissioning of the unacceptable antigens upload functionality which meant users must use APIs to update this information. A representative from HRSA asked about the decommissioning of the unacceptable antigen upload functionality and what brought this change on. Mr. McTier explained that this was an IT project to phase out this method of entry to move all vendors over to using APIs.

Mr. McTier presented the OPTN Computer System availability metrics to show that the matching function availability SLA is 99.9%, which excludes planned maintenance. During the reporting period there were eight occurrences of planned maintenance, and the actual downtime for each occurrence ranged from fifteen minutes to two hours and the actual downtime never exceeded the planned downtime that was communicated to OPTN members. OPTN Computer System availability exceeded the SLA for every month in the reporting period, except for February 2023 when there was an unplanned downtime of fifteen minutes. A committee advisor suggested shifting the OPTN Computer System availability metrics to look at the inverse, and measuring the events that occur with a decided threshold. This could shift the conversation for the NOOC to only look at months when downtime occurs in order to focus on areas of improvement. A representative from HRSA commented that it would be helpful to have the downtime events listed to provide transparency to the committee. The Chair responded that that information is available in the detailed report provided in the meeting materials and the information is broken down by planned downtime, unplanned downtime, full availability, and partial availability. Another representative from HRSA commented that this information should be provided in a dashboard. Mr. Nicholson explained that this information would be shared during the next NOOC meeting. Mr. McTier stated that the information provided to the committee is the information the Contractor is utilizing to develop these dashboards.

Mr. McTier presented matching function issues and explained how they are broken up into four different categories. Category 1 occurs when the entire match run system is unavailable, category 2 are issues where the system is partially available that affects all users of the system, category 3 occurs when there are problems with the system, but it only affects some users, and category 4 issues are issues affect one single candidate. Each category also has a resolution timeframe associated with them.

The final efficiency metric deals with policy revisions. Mr. McTier explained that this metric is based on programs reporting on each OPTN policy implementation and any revisions to these policies that were made after its implementation. During the reporting period, there were sixteen policy projects implemented, one project was revised due to policy adjustments, and seven policies were revised due to a programming defect.

When discussing timeliness metrics, it was explained that in 2016 the Board of Directors established a project delivery commitment for the implementation of Board projects. This metric said that 100% of projects must be completed within twelve months of their approval date by the Board unless the Board grants them a waiver. In the past, the Board has granted waivers to allow member organizations more time to prepare for a project, to expedite the implementation of another project, or because of an external dependency, such as OMB approval. Mr. McTier presented the median project delivery time from 2015 to 2022 that is included in the report. In 2022, the median policy project delivery timeline was 10 months.

When discussing usability, Mr. McTier presented on the OPTN Computer System Usability Survey which gathers feedback from OPTN members who use the OPTN Computer System and the use of their applications. The latest survey was conducted in May and June of 2022. Part of the survey asked members to rate their overall satisfaction with specific applications or elements of the OPTN Computer

System. The results from the survey showed that more than 90% of respondents reported a positive experience with the OPTN Computer System. A committee advisor asked if there was information as to why members selected anything other than satisfied or very satisfied. Amy Putnam, Director of IT Customer Advocacy, stated that some of the feedback they received was that people want more APIs, and users want more mobile options.

The final metric shared with the committee is the OPTN Computer System Capital Planning and Investment Control (CPIC) Score. This score is received each month from HRSA and measures the OPTN's responsiveness in addressing security related matters. The CPIC Score for the OPTN has been over 90 for 11 of the past 12 months, and 100% for 8 of the past 12 months.

Next Steps:

The Committee Chair concluded the presentation by asking if there were any additional metrics or data the NOOC would like to see in the report, that they should relay this feedback to Mr. McTier.

4. Security Project

Ms. Courtney Jett, Policy Analyst, began the conversation with the committee to discuss the security project, to report on the Accenture deliverables, and to discuss cybersecurity incident planning and what operational guidelines are included in this.

The OPTN is collaborating with Accenture Federal during portions of the security project implementation process. Ms. Jett explained that the committee will review the deliverables related to the operational rollout for attestations and audits at a future meeting and feedback will be incorporated from the pilot groups. Ms. Jett noted that due to feedback from the last meeting, the OPTN Contractor has considered staggering some attestation questions to focus on the most important areas first. It was noted that in terms of the budget, the proposed budget will be taken to the Finance Committee and then reviewed by the whole Board. Accenture recommended that there be eight full-time, in-house employees for attestations and 6 full-time employees for audits. The Contractor has considered both in-house staffing and contracting a third-party for this work. There is the potential for the Contractor to utilize Accenture for staff augmentation for incident management and security data calls at an additional cost. This information will be included in the FY24 budget review. The Chair asked if the Contractor would likely use in-house staff or contract a third-party to perform the work. Ms. Terri Helfrich, Director of Information Security, explained that the Contractor is leading more towards utilizing third-party contractors for the work to allow for a more efficient and quicker process.

The objective of the cybersecurity incident planning and the operational guidelines conversation was to begin developing operational guidelines for suspension and restoration of user and member accounts for the OPTN Computer System. These guidelines will allow the Contractor to better respond to security incidents as they arise and will guide what is allowed in policy language on appropriate actions for the OPTN and for the Contractor under the framework.

The operational guidelines already discussed with the committee were reshared. The guidelines are a priority to ensure every effort is made to continue the lifesaving work of transplant, a priority to ensure all threats are assessed independently as there is no "one-size fits all" scenario, priority to allow the OPTN Contractor to act on behalf of the OPTN in specifically prescribed circumstances by the NOOC, a priority to allow the OPTN Contractor to provide faster responses in certain urgent situations, and a priority for all incidents to still require NOOC review at the least retrospectively.

The committee discussed use cases based on requirements as it pertains to the Contract language. The Contract states that the Contractor shall support the NOOC in its effort to develop criteria for suspending both OPTN member organizations and OPTN member user accounts from the network. Ms.

Jett explained that in this case, the committee is discussing individual OPTN user accounts first and will then discuss OPTN member organizations. The NOOC is permitted to add or remove criteria over time as situations arise. The criteria that the committee had discussed prior were presented to determine whether these criteria were appropriate. The list of events that could result in temporary individual OPTN user account suspension could be due to a compromised OPTN account, an account local to member environment is compromised and the individual has an account to the OPTN Computer System or utilizes APIs with connectivity to the OPTN Computer System, the System of an individual who is a user of the OPTN Computer System or associated APIs is compromised by malware or ransomware and the compromise is limited in scope to their system, a member is notified of a compromise to a personal device used by an individual to access the OPTN Computer System, there is a violation of HIPAA Privacy laws, a confirmed data leakage by the individual has occurred, violations of OPTN Terms of Service have taken place, or a notification of stolen laptop for individual with access to the OPTN Computer System has been received (unless laptop encryption is in place and functional at the time of loss).

The Chair asked about the language on confirmed data leakage by an individual and whether this was the appropriate verbiage. They questioned whether the leak needs to be confirmed or just suspected for the OPTN to take action out of an abundance of caution. Ms. Helfrich responded that she did not have an issue changing the language but the issue with using the word suspected is figuring out where the investigation comes from when it comes to confirming whether a leak has occurred or not. A committee advisor commented that the language for this bullet is not enough to explain what the OPTN is looking for. After discussion amongst the committee, it was suggested that the language be changed to read "suspected/confirmed data leakage by the individual" to include both.

A committee advisor asked about suspending individual user access when a violation of HIPAA Privacy laws has occurred. They asked if this applies to any violation of HIPAA Privacy laws because they thought it was important to differentiate between unintentional and intentional violations. They suggested providing examples and levels of the type of violations. The advisor suggested that the current language is too vague, and users may not take it seriously. The Chair suggested that this be included to err on the side of caution and ensure there is no real threat before restoring a user's access.

Ms. Jett presented the criteria to suspend member access and to determine whether the listed situations were appropriate. It was noted that additional criteria may be added by the NOOC over time as situations arise. The situations that were listed where a member institution's access would be suspended included: an administrator's account has been compromised, a malware or ransomware attack identified and is systemic to the member organization, an indication of spread of malware with threat of spread to systems interfacing or supporting the OPTN Computer System, high or critical level Indicators of Compromise (IOCs) are identified within the environment and are not blocked and/or contained, identification of Advanced Persistent Threats in the environment, or identification of data exfiltration from the environment. The Chair asked how transplant would be interrupted at these member organizations if their access was removed. A committee advisor commented on the importance of contingency plans for each member organization to ensure transplant operations are not impacted if their access were suspended. The Chair commented on the high-level impact that suspension of use could have when a full member organization loses access compared to an individual user having their access suspended. A representative from HRSA asked about third-party access and the procedure to suspend access from these users. A committee advisor responded that it would be the responsibility of the member they are contracted with to assess the threat and determine whether a breach has occurred. The committee discussed potential actions to take if a third-party user is contracted by multiple members and what the protocol should be. A committee advisor suggested requiring members to submit information on who they have contracts with and what third-party users have access to the

OPTN Computer System. Ms. Helfrich informed the committee that the OPTN Contractor is unable to build a report based on third-party users to determine which members have contracts with certain users. A committee advisor commented that each member assumes the risk of their third-party contractors when they allow them to access the OPTN Computer System. The advisor stated that if something happens with a third-party member then the entire member's system needs to be taken offline until the issue is resolved. The Chair stated that it is important for these members to let the OPTN know if there is a breach within a third-party user, because other OPTN members could utilize the same third-party vendor.

After discussion from the committee, it was summarized that based on the committee's feedback, the NOOC might want to consider including a threshold on the number of users with compromised accounts with suspicious activity. The Chair responded that a certain number may not be the most effective way to handle this kind of issue, that it is important to give the Contractor some leeway to analyze the situation effectively. The Chair stated that it is important for the OPTN to notify members IT security contacts to make sure they are aware of the situation and are aware of all the information about the incident.

The committee then discussed re-enabling full member accounts and discussed what appropriate criteria would be for re-enabling a user after suspicious activity and how the OPTN can best communicate these criteria to OPTN members. Criteria that was proposed to the committee, dependent on the scope and criticality of the incident, included: approved third-party incident response vendor, law enforcement provides validation of restoration requirements provision of initial incident report, sections of the report related to OPTN access or interface points as well as system administration, establishment of a temporary, isolated environment with "bare metal built" systems, and proven remediation of prevention measures required are in place and operational. It was noted that additional criteria may be added by the NOOC overtime as situations arise.

A committee advisor asked if a template is given to members on what steps they need to adhere to in order to re-enable system access. Ms. Helfrich explained that members are provided with a member security checklist of essential items members must have in place that the OPTN has developed. The Chair stated that it is important for the OPTN to have conversations with the IT security contacts at the member organizations on what needs to be in place to bring them back online. They thought that these conversations could be useful to discuss how members can prevent such incidents and how to respond to incidents when they occur. The Chair cautioned on publishing a template on the criteria members need to have in place to come back online to the general public.

Ms. Jett presented a preview of an example on incident classification for the committee to discuss at an upcoming meeting as the committee will start on the classification system of what the OPTN's response action will be in terms of the maximum response action on the different tiers of criticality. The committee was asked to consider the example for their next meeting and consider different response actions.

For the next meeting, the committee was asked to consider the question of who should approve the threat level of an incident to determine appropriate action. Ms. Jett explained that some actions could be delegated to the OPTN Contractor, some to a NOOC subgroup, the NOOC Chair, or to HRSA. The committee was asked to consider what actions they thought were appropriate to delegate to the different groups and bring their thoughts to future discussions on the matter. The Chair commented that this conversation is important for the NOOC and HRSA to give some delegation to the OPTN Contractor to act in given situations. They continued that they find it hard to think of a situation when the committee would not trust the experts and subject matter experts of the OPTN Contractor when handling these situations. A committee advisor commented that they agreed with the Chair's approach.

A representative from HRSA asked to revisit who from the member organizations should sign the institutional self-attestation. Ms. Jett explained that currently, the person responsible for this would be the information security contact, but in policy language it is not specified who should sign these forms or who is responsible for signing these forms. The representative from HRSA then asked who is typically responsible for the information security content at member institutions. Ms. Jett explained that this is a new role being developed in the new policy. The Chair explained that the NOOC decided it was up to members to determine who they would like to delegate as their security contact because it could be a different person for different member types. They commented that this person is not necessarily just a transplant staff member and that each member's organizational delegation is going to look different from one another, but ultimately they are signing on behalf of the member. The representative from HRSA asked if anyone other than the security contact needed to be aware of the relationship and responsibility between the member and the OPTN; they asked that this responsibility be clear in policy language. Ms. Jett explained that this is not a practice for any other OPTN policies to state who at an institution must sign the forms. The representative from HRSA commented that they thought this situation might be different because there is an institutional commitment being made. The Chair asked how the OPTN would operationally be able to enforce this. HRSA asked to discuss this more in the future. A committee advisor stated that they were uncomfortable with the terminology being used and worried about site administrators being the primary contact for this given situation. A representative from HRSA commented that typically, this person would be the Chief Information Officer (CIO) title at each member organization, but if there is someone else the NOOC thinks should be in this role, HRSA would be open to consider their suggestion.

The meeting was adjourned.

Attendance

- **Committee Members and Advisors**
  - Adam Frank
  - Bruno Mastroianni
  - Clifford Miles
  - Daniel Yip
  - Ed Hollinger
  - James Pittman
  - Jeff Sterrette
  - Kelley Hitchman
  - Paul Connelly
- **HRSA Representatives**
  - Adriana Martinez
  - Adriane Burton
  - Arjun Naik
  - Christopher McLaughlin
  - Cliff Myers
  - Manjot Singh
  - Vanessa Arriola
  - Vinay Vuyyuru
- **UNOS Staff**
  - Amy Putnam
  - Anna Messmer
  - Bridgette Huff
  - Courtney Jett
  - Jason Livingston
  - Jonathan Moore
  - Kristine Althaus
  - Krissy Laurie
  - Laura Schmitt
  - Liz Robbins Callahan
  - Marty Crenlon
  - Matt Belton
  - Michael Ghaffari
  - Morgan Jupe
  - Rebecca Murdock
  - Rob McTier
  - Roger Vacovsky
  - Susie Sprinson
  - Terri Helfrich
  - Tiwan Nicholson
  - Tynisha Smith