OPTN Network Operations Oversight Committee
Meeting Summary
November 15th, 2022
Webex

Edward Hollinger, MD, PhD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 11/15/2022 to discuss the following agenda items:

1. Welcome
2. OPTN System (UNet) APIs
3. VCA Incorporation into the OPTN System
4. Real-time UNet Availability Demonstration
5. 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 committee's discussion about the network security project. The committee will also discuss other updates around the OPTN Computer System.

2. OPTN System (UNet) APIs

Marty Crenlon, Healthcare Integration Program Manager, presented on the current OPTN Computer System's APIs. Mr. Crenlon spoke about the API dashboard on the donor data and candidate data, separated by transplant centers and OPOs. Mr. Crenlon spoke on the driving approach behind API adoption. Some aspects of this approach include adding more APIs, targeting specific APIs, targeting specific members, and increasing adherence. Mr. Crenlon also detailed the near-term engagement activities from the different membership organizations.

In 2023, there are three new APIs additions happening, including the organ check-in API, deceased donor creation API, and deceased donor HLA submission API.

Summary of Discussion:

HRSA asked for clarification on the graphics displayed in the presentation; they asked if the green cells represented full API adoption or only some API adoption. They expanded their question and asked if the OPTN can identify why some centers choose to use one set of APIs and not another. Mr. Crenlon explained that the colors of the graphics were green and red due to the evaluation process that APIs follow. It is a "yes" or "no" measurement for API use in organizations.

One committee advisor asked about transplant centers, and if it were possible to classify which transplant databases each center utilizes. Mr. Crenlon responded that the OPTN is able to pull this information and that the OPTN has visibility as to when transplant centers are integrating APIs.

HRSA asked if the NOOC could focus on integrating existing APIs across member organizations before looking to add more APIs to the system. They also asked that the OPTN provide more information on

what the new APIs would be for member organizations. Mr. Crenlon explained that the conversation of adopting APIs versus what is driving API adoption, are driven by separate resources. He detailed the different vendors and contacts that are utilized during each respective process. HRSA commented that they did not think adding more APIs would be effective if members did not understand the adoption around the new APIs. They recommended the OPTN reach out to members for their feedback on new API adoption. They think the OPTN could focus on targeting the existing APIs first, then communicate the need for the new APIs and who the consumers of the new APIs are. Mr. Crenlon said they are able to provide information on new APIs ahead of time to their software engineering team.

Another representative from HRSA asked if the OPTN had API adoption plans from each of the member organizations that have not yet adopted APIs. They suggested this could be a useful tool so there is documentation of the timeline and so someone is able to follow up on the progress of a member's API adoption. Mr. Crenlon explained that there is not currently a process like this because members are not required to adopt APIs. Two HRSA representatives said that although API adoptions are not mandatory for members by contract, they would like to see as high a level of adoption from members as possible. They stated to the NOOC that the ultimate goal of APIs is to reduce the burden of data collection for members. HRSA thought there should be more encouragement for members to fully adopt APIs. A committee advisor responded to HRSA that if APIs are not mandatory, then a lot of members are not going to adopt them. They continued that if HRSA wants 100% adoption by member organizations than adoption needs to be made mandatory and that it is then up to the OPTN to execute this mandate.

Next Steps:

Mr. Crenlon will distribute dashboard metrics to the committee following the meeting via email. Dr. Hollinger tasked the committee to think about possible barriers when it comes to API adoption. He asked the committee to consider the barriers for members that may not use APIs at all and for members that do utilize APIs and what aspects of APIs do they find most valuable to their organization.

3. VCA Incorporation into the OPTN System

Amy Putnam, Director of IT Customer Advocacy, informed the committee of the recent change in incorporating VCA into the OPTN Computer System. Ms. Putnam stated that the original plan was to release the waitlist for uterus in March because uterus has the highest volume compared to other VCA organs. Thus, the remaining nine organs were planned to be released in May, just two months later, with the rest of the system.

Ms. Putnam explained that due to the changes by the OMB in reporting race and ethnicity, implementing two different styles of data collection back-to-back did not make sense. Therefore, the OPTN's updated plan is to release all VCA critical components at the same time in May 2023.

Summary of Discussion:

HRSA asked if changing race and ethnicity could be implemented as a microservice. UNOS staff explained that software engineers are building this pattern on the way race and ethnicity is implemented and this model is shared throughout VCA implementation.

4. Real-time OPTN System Status Page Demonstration

Tiwan Nicholson, Director of IT Operations, presented on the real-time OPTN system status page to the committee. The purpose of the system status page is to inform the user community on system availability, outages, planned maintenance, and other miscellaneous system details. The system status page is a requirement of the OPTN contract to help promote visibility and transparency within the OPTN

systems. The presentation detailed the frequency of status updates by category and showed an example of an incident announcement to the committee.

Summary of Discussion:

HRSA asked if users are only able to access this page on the UNOS website or if it is accessible from the OPTN Computer System. Mr. Nicholson explained that because project is still in the pilot stage, that the page is not currently accessible from the OPTN Computer System. He noted that the team is working to identify the proper places for this information to exist. HRSA thought it may be confusing for someone to go to the UNOS website to find out information for the OPTN Computer System. They continued that per the contract, HRSAs understanding is that this program should be available in the OPTN Computer System. Mr. Nicholson concurred that this information could live in multiple places to ensure that members are able to retrieve this information successfully.

5. OPTN Member Information Security Policy and Bylaw Enhancements

Rebecca Murdock, Senior Policy Counsel, updated the committee on feedback received on the security enhancement language. The committee was provided a detailed, edited copy of the proposal for their review prior to the meeting. The objectives of the conversation were to focus on the three main OPTN member types and to reach a consensus on topics such as access control and training, incident management response and security framework.

When discussing access control, the committee discussed how members were to gain and retain access to the OPTN Computer System and the requirements they must adhere to. The conversation of access control also led to discussing the requirements for site security administrators and their role.

The committee deliberated on what an appropriate framework could be when it comes to incident management responses. The committee's goal of the conversation was to develop a process and timeline for OPTN members for reporting security incidents to the OPTN, and then to HRSA. Committee members also discussed the incident response plan and what they thought this should look like for OPTN members.

The committee was remined that this project is a large undertaking and can be done in phases of implementation because of the depth of detail and information this conversation requires. The committee also discussed who should perform audits if the OPTN decided to mandate audits, or whether proof of an audit was proficient enough.

Summary of Discussion:

Dr. Hollinger asked about the information on the availability of auditors and what the cost associated with this may be. UNOS staff responded that auditors are available to audit various frameworks, but it is difficult to estimate a price because cost is contingent upon the size of the organization and the system they are auditing. Dr. Hollinger asked if for larger organizations, these audits are already being completed across their organization, then this could be one small portion incorporated into the organizations larger audit. A committee advisor recounted his experience recently on receiving quotes from third-party auditors and received roughly the same quote from them all. They said that maturity of the organization is also considered by third-party auditors. Dr. Hollinger noted that clarification would be necessary on whether or not audits must be performed by outside organizations or if internal auditors would be acceptable. He asked if member organizations could anticipate the OPTN Contractor requesting access to audit materials.

A committee member asked how they would determine whether a member passes their audit or not, and what happens if they do not pass. A committee advisor said that when audits are completed for

HIPAA then the organization must demonstrate to CMS that they are improving every year. They said that organization don't necessarily receiving a passing grade.

A visiting attendee said that their own organization is stricter on themselves than outside vendors. They asked if there were a way for members to demonstrate that their security system is adequate, so organizations do not have to prove this when mandated. They suggested the committee consider an organization's level of security, and that if an organization has ample security, then they may go longer periods without mandated audits. They noted that most members likely exceed these standards, and they worry this would just create busy work for these member organizations. Dr. Hollinger commented that the other challenge the NOOC faces is that they do not have a comprehensive idea of what a baseline of security is across the different member types. He suggested the committee pose this question to the community during public comment to better understand what the baseline may be. Dr. Hollinger continued and agreed that many members will meet the standards and beyond, but the organizations that will need more attention are the organizations that are just getting started in their security journeys.

A committee member asked if the OPTN were able to contract a single, third-party organizations to perform audits on all members to understand a baseline standard. They thought this would be wise to ensure audits are standardized and uniform. Dr. Hollinger thought the first step should be self-auditing and to have questions from the NOOC guide these audits.

HRSA asked whether self-attestations were reasonable for member organizations to gain and retain access control. Ms. Murdock explained that self-attestations could be used as a piece of an audit, but the question remains how the OPTN would monitor this. This led to the question of who should be completing these audits and who is performing these audits on behalf of the OPTN. One committee member said they thought the OPTN should partner with a third-party to complete these audits. They thought it would be wise to complete random audits, and then have audits when there are changes within a member's system. One committee advisor thought it was wise to recognize that transplant hospitals are going to meet the standard the OPTN sets, but the burden is going to land on smaller OPOs and labs.

With this suggestion in mind, Ms. Murdock asked the committee whether the committee would like a frequency of the audits be defined in the policy. One committee member commented on the importance of the language to say that the results from the audit could be provided to the Contractor upon request. This could allow member organizations to hire their own third-party vendor to perform their audits, but the information still be provided to the Contractor.

A committee advisor thought it was important to make the distinction between an audit and an assessment of a member's system. They thought it was important to differentiate between audits that are performed because there is a concern about a member's system, then there are standard trust audits that are performed to ensure members are utilizing the OPTN Computer System responsibly. They thought hospitals would not have any issues meeting these requirements, whereas smaller member organizations might have a difficult time ensuring their system meets the requirements.

When the committee was asked how frequently members should submit attestations, there were differing answers. A committee member thought that an annual attestation was appropriate. A committee advisor recommended attestations be completed when a member signs a new information security agreement, but if nothing within their system has changed, then members should not have to complete an attestation annually. This seemed redundant if nothing within the member's system has changed or if the requirements from the OPTN have not changed. Ms. Murdock asked whether annual audits were appropriate or if there was another timeframe that seems more appropriate for

organizations. A committee member said that if there were no changes in the ISA then there was no reason for these systems to be retested.

When discussing site security administrators, a committee member asked what would happen if only one person from their organization doesn't complete their training, but the rest of the organization has. Ms. Murdock explained that there is a difference in violating a policy versus violating the data or the system itself. She noted that completion of the training is a member obligation but would not be a threat to the system to grant one person access who has not completed their training. She reassured the committee that this is a topic they will discuss in more depth later. A committee advisor asked the committee to consider when someone has access to multiple systems, what would happen if one of their organization's access was revoked. UNOS staff explained that each user has a home institution where they originally receive access, and this is who would ultimately have control over their access. Staff noted that this is a question they have also been discussing and working to address. A committee advisor wanted to make sure this question was discussed so site administrators are aligned when it comes to questions of access for users that work for multiple member organizations.

When discussing the incident response plan, a committee member asked if the type of device they are using matters in terms of posing a threat to the system. They thought that not all devices required the same amount of scrutiny. They wanted to know if there were different standards depending on the device. UNOS staff asked if there were general use agreements for members using their personal mobile devices to access the OPTN Computer System. A committee advisor answered yes, that for most organizations, there is a requirement that member security software be uploaded to the device.

The committee discussed if within one hour was an appropriate time window to notify the OPTN of an incident. A committee member thought it was important to consider what an incident was and what situations this covered. They thought this understanding was important so the OPTN is not overwhelmed by reports of incidents that are not necessary to report. Multiple committee advisors worried about the time limit members had to report an incident to the OPTN. The proposed language said that members had one hour to report an incident to the OPTN. Committee members thought this was an unreasonable amount of time. A committee advisor explained that IT security within these organizations will know about an incident hours before someone within the transplant department may know. They thought it was important to consider that this kind of information is not disseminated instantaneously throughout an organization. Another committee member agreed that during these incidents, their area of the hospital is low priority on relaying information to and so they believed the one-hour timeframe was unreasonable. Another committee advisor thought that it was important to remember that organizations will likely keep these situations as confidential as possible to ensure there is no undo stress throughout the organization. These members will also want to take care of the issue as quickly as possible and the people that would be notifying the OPTN are likely the ones actively working to neutralize the incident.

A committee advisor suggested that educational materials be available to members. These materials would be crucial to inform members on how to accurately report incidents to the OPTN and ensure standards are followed. Ms. Murdock stated that a point of contact is important for each organization to have when communicating with the OPTN. She posed the question to the committee on whether this is duplicative of the site administrator role. The committee discussed whether or not it was reasonable for the point of contract to report incidents to the OPTN within an explicit timeframe; the committee acknowledged the potential difficulty in monitoring this.

Dr. Hollinger asked the committee to go back to their respective organizations and see if there are lists of people that organizations notify when a security incident occurs, or to learn how their organization notifies people. Dr. Hollinger said that if the OPTN Contractor wants to be a party on that list, then the

committee members should figure out how these lists are created and how the OPTN Contractor could be added. A committee advisor stated that their organization does have a list of people to notify, and their list is prioritized to most crucial and disseminates from there. Ms. Murdock suggested the committee present incident notification during public comment to receive feedback on how the notification process can be more efficient.

Dr. Hollinger asked Ms. Murdock to send the slides out to the committee for their review to bring back questions and feedback on the proposed language.

NEXT STEPS:

Committee members were asked to consider their organization's notifications processes when it comes to incident or risk notification to potentially affected parties. Committee members were asked to review the meeting slides and proposed language ahead of their next meeting.

Upcoming Meetings:

- November 30th
- December 12th
- December 16th

Attendance

- **Committee Members and Advisors**
  - Bruno Mastroianni
  - Clifford Miles
  - Daniel Yip
  - Edward Hollinger
  - James Pittman
  - Kelley Hitchman
  - Kimberly Rallis
  - Maryjane Farr
- **HRSA Representatives**
  - Adriana Martinez
  - Adriane Burton
  - Arjun Naik
  - Chris McLaughlin
  - Clifford Myers
  - Demonique Lewis
  - Satish Gorrela
  - Vanessa Arriola
- **UNOS Staff**
  - Alex Tulchinsky
  - Amy Putnam
  - Anna Messmer
  - Angel Carroll
  - Bonnie Felice
  - Bridgette Huff
  - Liz Robbins Callahan
  - Marty Crenlon
  - Michael Ferguson
  - Michael Ghaffari
  - Morgan Jupe
  - Rebecca Murdock
  - Rob McTier
  - Roger Vacovsky
  - Susie Sprinson
  - Taylor Livelli
  - Terri Helfrich
  - Tiwan Nicholson
  - Tony Ponsiglione
- **Other Attendees**
  - Jason Huff
  - Nancy Metzler
  - Susan Zylicz