OPTN Network Operations Oversight Committee
Meeting Summary
May 17, 2024
Webex

Daniel Yip, MD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 5/17/2024 to discuss the following agenda items:

1. Welcome
2. Member Security Metrics
3. Member Security Attestations & Audits
4. Revise Conditions for Access
5. Network Operations Metrics and Monitoring Report
6. Closed Session

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

1. Welcome

Dan Yip, Chair of the Network Operations Oversight Committee (NOOC), welcomed committee members and advisors and provided an overview of the agenda.

2. Member Security Metrics

Terry Doolittle, Member Security Program Manager, presented member security metrics on the first wave of attestations. Mr. Doolittle asked the committee to consider any desired changes to the program based on member responses and to consider support members may need for the next two waves of attestations. Mr. Doolittle reviewed the background of the first wave of attestations with the committee, and shared that the OPTN reviewed overall attestation scores based on questions, criticality, and member type. Mr. Doolittle presented the compliance distribution based on these characteristics. Committee members discussed members that submitted all answers as "not applicable".

Mr. Doolittle presented the metrics by control group and shared the implementation percentage by control group. He explained that it is important to analyze the metrics by control group because while some members performed worse in certain control groups, they did not consistently underperform across multiple control groups, making the scores more balanced overall. While analyzing the metrics by control, Mr. Doolittle explained that they highlighted all controls that were one standard deviation below the mean for percentage of members who had them fully implemented and explained that the plan is to review implementation status by member type and type of implementation. Mr. Doolittle highlighted some of the critical controls in place. Mr. Doolittle asked the committee to consider whether there are explanations for why members may not have specific controls fully implemented, whether there are ways for the OPTN to aid members to fully implement these controls, and whether there are any controls that the committee believes should be required for members to implement in their second year of attestations.

<u>Summary of Discussion:</u>

The committee discussed how to encourage members to submit their attestations, and discussed whether there was benefit in comparing similar members and their attestation results. The committee also discussed whether they should create benchmarks for members during the first round of attestations. Committee members suggested explaining to members that the first year of attestations is to record a baseline for members, and that members are encouraged to submit their attestations to receive feedback from the OPTN to enhance their system.

The committee also discussed how to measure a standard deviation of members when analyzing attestations, and they discussed whether there should be a formal way for members to submit feedback to the OPTN on their attestation experience. The committee discussed specific metrics by control and considered why some members may not have specific controls in place. Committee members discussed that some members may not have specific controls in place due to their size, their member type, their location, or other factors.

Next steps:

Mr. Doolittle shared that the second wave of attestation metrics will be provided to the NOOC once they are completed.

3. Member Security Attestations and Audits

Mr. Doolittle presented on member security attestations and audits. Mr. Doolittle shared that the goals of the topic were for the committee to discuss the timing for audit implementation, the required actions for gaps, and the operational needs for audits.

Mr. Doolittle shared the member audit timeline. Mr. Doolittle asked the committee to consider whether members should be required to respond to gaps found during an audit, whether there should be a minimum level of compliance with NIST 800-171 (rather than being required to remediate all gaps) and asked them to consider a potential rollout to members for minimum compliance.

Mr. Doolittle then presented on attestation and audit timing. He asked the committee to consider whether new members applying to the OPTN should be required to complete their attestation prior to being granted access to the system, and whether member should be required to complete an attestation during their audit year. Mr. Doolittle also asked the committee to consider audit operationalization and whether audits should be performed in-person or virtually.

Summary of Discussion:

When discussing required actions for gaps, the committee discussed the policy language and discussed whether there is specific language on actions for gaps. Contractor staff explained that although there would be audit findings, the NOOC would need to decide whether members need to make revisions on their identified gaps. The committee discussed whether there should be different timelines for members to remediate their gaps depending on the critically of the control.

The committee discussed attestation and audit timing for members. The committee chair suggested that members perform their attestation every year, even if it is their audit year.

4. Revise Conditions for Access

Courtney Jett, Policy Analyst, presented on revise conditions for access to the committee. Ms. Jett shared that the goals of the discussion were to review the feedback received from the Data Advisory Committee (DAC) on the project, and to discuss outstanding project and timeline questions. Ms. Jett reminded the committee what the overall proposal is to accomplish. She noted that the proposal will:

- Require OPTN membership as a condition of access to the OPTN Computer System and reduce potential barriers to OPTN business membership
- Limit reasons for access to the OPTN Computer System to facilitating organ transplantation, fulfilling OPTN obligations, and quality assurance and performance improvement (QAPI)
- Defining OPTN Data and require reporting for privacy breaches of OPTN Data
- Require all members who access the OPTN Computer System to execute a Data Use Agreement (DUA) with the OPTN
- Require all members with system interconnections to the OPTN Computer System to develop an Interconnection Security Agreement (ISA) with the OPTN
- Require OPTN business members who access the OPTN Computer System to follow the same information security requirements that apply to other member types who access the OPTN Computer System.

Ms. Jett shared feedback the project received from the DAC and noted that the committee was supportive of the general concept of additional protections for OPTN Data and the OPTN Computer System. Ms. Jett noted that the committee emphasized that business members need to be required to complete a DUA and the DAC wanted more detail on how this will be executed. Ms. Jett also shared that the DAC asked to review the draft DUA and policy language. Ms. Jett noted that the DAC shared that OPTN members will likely want to redline the DUA and noted that the NOOC should consider what level of changes would be permitted. Ms. Jett shared that the DAC discussed how often members should have to renew their DUA; Ms. Jett shared that three years is the maximum timeframe under NIST 800-53 standards but that the current NOOC recommendation is a one-year renewal period. Other feedback from the DAC included their involvement in the drafting of the DUA, considerations on ownership of OPTN Data once incorporated into medical records, considerations on prohibited uses of OPTN Data access through the OPTN Computer System, and considerations on how to ensure the OPTN DUA will apply to everyone accessing OPTN Data at member organizations, even if they are not employed by the member organization.

Ms. Jett presented on the policy language for reporting privacy breaches. She shared that the goal of reporting privacy breaches is to ensure OPTN Data is secure, whereas the goal of the current policy requiring reporting of security incidents is to ensure the OPTN Computer System is secure. Ms. Jett shared a draft definition of privacy breach based on the NIST definition. Ms. Jett asked the committee to consider how long members should have to report privacy breaches of OPTN Data that occur at their organization, and to consider whether members should only be required to report confirmed privacy breaches.

Ms. Jett then presented on QAPI uses of OPTN Data, and asked the committee to consider whether members should be permitted to access all historical OPTN Data for QAPI purposes or if they should only have access to data going back a certain number of years. If the NOOC decided members should only be able to access data going back a certain number of years for QAPI purposes, then they were asked to consider the appropriate timeframe.

Ms. Jett presented on reviewing business members reasons for accessing the OPTN Computer System. Ms. Jett explained that because reasons for access to the OPTN Computer System will change, there will need to be a review period in place to ensure appropriate access for all business members to the OPTN Computer System. Ms. Jett noted that the NOOC should consider how long members should be permitted to submit their explanation of reasons for access to the OPTN Computer System. Ms. Jett then presented a proposed plan for the NOOC to review pertaining to business members accessing the OPTN Computer System.

Ms. Jett presented the proposed business member transition period. Ms. Jett noted that the ISA timeline would allow members 6-12 months to complete their ISA, based on previous discussions the committee had that 6 months may not be a sufficient amount of time for some members to complete their ISA.

Summary of Discussion:

When discussing reporting privacy breaches, the committee discussed that the HIPAA requirement is 60 days to notify HHS. The committee decided to wait to make a decision on how long members had to report privacy breaches until the definition of OPTN Data is established.

When discussing QAPI uses of OPTN Data, committee members commented on the length of time that members should be permitted to go back and access OPTN Data. Many committee members commented that going back too far in time would not be relevant to members, therefore, they did not see a need for members to go back further than five years. A committee member commented that OPTN members should be able to access OPTN Data for as long as a program has been in existence, while another committee member suggested that OPTN members should be permitted to go back twenty years to access OPTN Data. The committee did not determine the length of time members should be permitted to go back and access OPTN Data.

When discussing business members' reasons for access to the OPTN Computer System, a committee member commented that the time members have to submit their explanation should differ depending on if they are an existing member or a new member. Ms. Jett explained that new members would not receive access to the OPTN Computer System until their application is reviewed, so therefore the NOOC is asked to consider how long existing members should have to submit their explanation. A committee member asked if this is a one-time explanation for business members. Ms. Jett commented that the NOOC could decide whether a member needs to submit a new explanation on access depending on if their reason for access has changed. A committee member suggested that there be a periodic review of business members' reason for access. A committee member suggested that OPTN members should have three months to submit their explanation and that they should specify that if a member changes or adds a business line, then they must resubmit their reason for access.

The committee discussed the possibility of the proposal going out in two parts as they are awaiting feedback on the definition of OPTN Data and proposed DUAs. The committee chair suggested that the committee move forward with the privacy and reporting component of the proposal so as not to delay. Ms. Jett noted that the committee will be asked to vote on policy language during their next meeting to submit for Summer 2024 public comment.

Next Steps:

The committee plans to review and vote on policy and bylaw language for Summer 2024 public comment during their next meeting. The proposal will include all components discussed around conditions for access, except DUAs and uses of OPTN Data, which are pending review from HRSA's legal team. The two items currently undergoing HRSA legal review will be submitted for public comment at a later date.

5. Network Operations Metrics and Monitoring Report

Rob McTier, Business Architect, presented the network operations metrics and monitoring report. Mr. McTier explained that the metrics and monitoring report covers a 12-month reporting period, from April 2023 to March 2024, and is a contract deliverable. Mr. McTier also presented the development of new metrics and what the committee could anticipate during the next monitoring period, including additional contract requirements and metrics on member system security.

Mr. McTier shared the performance metrics within the report, including metrics on availability and uptime, request rate, error rate, and latency of the OPTN Computer System. Mr. McTier also presented information on system reliability and performance metrics, and member security metrics. Mr. McTier asked the committee to consider what the metrics indicate about the performance of the OPTN Computer System, how the performance of the OPTN Computer System could be improved, and how the metrics themselves can be improved in the future. Mr. McTier highlighted specific metrics to the committee, including match run time, organ offer notification time, what OPTN Data can be submitted through APIs, what API projects are currently being worked on, OPTN Computer System Availability, matching function issues, policy implementation revisions, policy project implementation performance, median policy project delivery time, UNet usability survey, and the CPIC score of the OPTN Computer System.

Summary of Discussion:

The committee discussed trends seen throughout the different metrics and discussed whether there are significant trends to note. The committee also discussed the UNet usability survey, API adoption across different member types, and the requirements set by the contract for OPTN Data to be submitted using APIs.

6. Closed Session

The committee met in a closed session.

The meeting adjourned.

Attendance

- **Committee Members and Advisors**
  - Andrew Kao
  - Bruno Mastroianni
  - Colleen McCarthy
  - Daniel Yip
  - Edward Hollinger
  - Kelley Hitchman
  - Paul Connelly
- **HRSA Representatives**
  - Adriana Alvarez
  - Arjun Naik
  - Christopher McLaughlin
  - Steve Keenan
  - Vinay Vuyyuru
- **UNOS Staff**
  - Anna Messmer
  - Courtney Jett
  - Kimberly Uccellini
  - Lindsay Larkin
  - Liz Robbins Callahan
  - Michael Ghaffari
  - Morgan Jupe
  - Rob McTier
  - Sevgin Hunt
  - Terry Doolittle