OPTN Network Operations Oversight Committee
Meeting Summary
November 30th, 2022
Webex

Edward Hollinger, MD, PhD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 11/30/2022 to discuss the following agenda items:

1. Welcome
2. Predictive Analytics Technical Review
3. 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 to committee's discussion about the network security project.

2. Predictive Analytics Technical Review

Michael Ghaffari, Director of Software Engineering (UNOS), presented an update to the committee on predictive analytics. Mr. Ghaffari discussed the different collaboration phases the project has undergone, with the project currently in the third phase. The third phase includes the implementation of beta and pilot testing on real offers in OPTN Donor Data and Matching System. The presentation then discussed the national view of predictive analytics which considers customer feedback on the project. The software architecture recommendation was also explained in terms of Azure Databricks that have been utilized throughout the development of the project.

Cloud native platforms have been an asset to the project and have given the project ideal capabilities; these include guaranteed message delivery through Service Bus, self-healing Azure Functions, and demand-based scaling and bursting for consistent performance. These operational processes show how the predictive analytics interact with one another, with the goal of ensuring that at the time of the match, they can send the information into Azure (the cloud native environment) then store the information and process it into live visuals for decision makers.

The Azure Dashboard has allowed for the quick monitoring of key situations such as API availability for predictive analytics, the time it takes to process a predictive analytic for a specific candidate, and the failures added to the dead letter queue.

Mr. Ghaffari concluded the presentation by detailing the timeline for the national rollout of predictive analytics.

Summary of Discussion:

A representative from HRSA asked what examples were applied to the analytic for the machine to learn and the architecture used. They also asked if HRSA and Mr. Ghaffari could go into more depth about APIs. The HRSA representative asked for clarification on what stage the project is currently in. Mr.

Ghaffari explained that the project is currently in the pilot, and it has been developed to process all adult kidney matches in a cloud native environment that has no impact on the OPTN Computer System. The system is built in this way, so the system is handling all the adult kidney matches and the developers can monitor through their dashboards to obtain a confidence ahead of the national release.

HRSA asked to have a technical deep dive session to understand the predictive analytics architecture that has been discussed. The group agreed to discuss this during a future COR call.

3. OPTN Member Information Security Policy and Bylaw Enhancements

Rebecca Murdock, Senior Policy Counsel, reintroduced the project and the progress since last meeting. The objective of the meeting was for the committee to reach a consensus on the approach to security framework and incident management response and how they apply to member hospitals, labs, and OPOs.

Last meeting, the committee agreed that OPTN members should be able to use any framework that meets the OPTN requirements and adheres to an industry standard security framework. The committee discussed possible security frameworks in more detail to address attestations, routine audits, and administrated exams. Attestations are important to monitor member compliance with the security framework and to establish a timeline for members.

During the last meeting, the committee briefly discussed the importance of incident management response. During the meeting, they discussed the possibility of notifying the OPTN of security incidents occurring on any device that connects to the OPTN Computer System or the device by which a member provides information to the OPTN. The committee also discussed what an appropriate timeframe was for members to report a security incident to the OPTN.

Summary of Discussion:

When discussing security frameworks and having the OPTN maintain a list of approved security frameworks, the committee thought that this list would be an addendum so it could be edited over time. HRSA asked if the language would identify a point in time when these terms would be effective by, to which Ms. Murdock confirmed that dates will be identified to tell users when a protocol becomes effective. This topic led the committee into discussing what this meant in terms of attestations and how the OPTN would monitor these attestations. Another representative from HRSA asked if there is going to be a level of maturity that is expected with each framework and how this would affect institutions adherence to the different frameworks. They asked if members would have to adhere to all the controls stated in the frameworks, or if there is a certain percentage or level of adherence they must reach. A committee advisor agreed that this question of maturity and controls is important in measuring a member's success in achieving a framework. A committee member asked if there were any industry standards the committee could review as guidance when it came to a measurement of success. When discussing maturity levels, Ms. Murdock encouraged the committee to pose this question to the community during public comment. She informed the committee that when discussing adherence to a framework this does coincide with monitoring and enforcement, which the committee plans to discuss next meeting. A committee advisor suggested education to members on what the framework looks like and how it's scored. They expressed their concern over the difficulty the OPTN may experience when trying to score frameworks. A representative from HRSA asked how they would determine which framework was best suited for a member institution. They suggested the OPTN create a checklist for members to use to demonstrate why they are using a specific framework. Ms. Murdock suggested creating a draft list to have the committee review or even submit for feedback during public comment. A HRSA representative suggested the committee consider choosing different control families and what

controls are associated with each family. They also suggested that the list of necessary controls could increase as a members maturity level increases.

When discussing attestations, a committee member asked the group to consider whether a member's maturity level could factor into the frequency of attestations. They suggested that if a member demonstrates that their system is mature and they're excelling with their security, then their attestations don't have to be as frequent as a member who continues to struggle to meet the criteria of their framework. They also suggested that for members struggling to meet the criteria, have the OPTN guide them and educate them in the process. A committee advisor suggested consistency when it comes to attestations, so members adhere to a checklist. They thought there was risk no matter how mature a system is and did not think maturity level should impact a member's attestation frequency. A representative from HRSA thought that a frequency of less than a year was not realistic unless the member is at a high level of maturity. A committee member suggested the OPTN analyze attestations but also examine a member's other controls in their system to allow members to grow and mature their systems.

When discussing the audit, a representative from HRSA had the idea that an auditor could use the attestation checklist within their audit. They suggested that there be two events for members: the attestation and the audit, which will each be performed at different frequencies.

The committee decided that yearly attestations for all critical points of the system would be appropriate and have rotating criteria that are spaced out over a span of three years to be examined during their yearly attestation. When it came to deciding the frequency of audits, representatives from HRSA thought it would be a best practice to use three-year audit frequency. They expressed this as a best practice to keep things consistent for members. The committee also discussed the possibility of auditing a program more frequently than three years if there are any concerns around their system, but no less than every three years.

When discussing incident management response, the committee discussed whether notification was necessary for just a confirmed incident or event, or if notification to the OPTN is necessary for even a potential threat. The group discussed what the definition of "confirmed" is in these situations, to which a representative from HRSA explained that from a cybersecurity perspective, there is a process where one would declare something an incident rather than an event, and there is a designated person to make this declaration. HRSA stressed the importance of the terminology in this portion of the policy because in the past, members did not self-report because they were unsure which events or incidents they were expected to report. Ms. Murdock stressed that this portion of the policy is to apply to incidents that have been confirmed to have happened and could potentially affect the OPTN Computer System. Member institutions should have a single point of contact with the OPTN, therefore this person would be well-versed on what kind of incidents or events need to be submitted to the OPTN. A committee advisor expressed their concern with reporting times to ensure that the OPTN is notified as soon as possible in order to minimize the risk to the system. The committee held a robust conversation on whether to use the word confirmed because they worried people may hesitate to report if they misunderstand the OPTN's meaning of the word confirmed. Multiple members of the committee suggested deleting the word confirmed from the policy language to avoid any confusion.

When discussing the definition of incident, HRSA thought that this could be easy to define if each organization had an incident response plan in place, because within each plan there should be a definition of an incident. Ms. Murdock worried that community members and members of the general public may not have as easy of a time defining what an incident is, so it is important to have a common definition of the word for the sake of this policy. HRSA recommended using the NIST definition of an incident, so they do not have create a separate definition.

Committee members were asked to consider the ideal timeframe for reporting security incidents to the OPTN. The committee discussed the possibility of having a one-hour time frame to notify the OPTN of any incidents. A committee member suggested members should report as soon as possible but no later than 24 hours after learning about the incident. A committee advisor thought that because the policy planned to clearly define what an incident entails, that reporting within 24 hours was an appropriate timeframe.

NEXT STEPS:

HRSA asked to table the conversation about notification to the OPTN of security incidents to ensure that what the OPTN was requiring lined up across other government entities.

Next meeting, the committee will discuss the incorporation of other users through member access into obligations, and the committee will discuss what monitoring looks like.

Upcoming Meetings:

- December 12th
- December 16th

Attendance

- **Committee Members and Advisors**
  - Adam Frank
  - Bruno Mastroianni
  - Clifford Miles
  - Daniel Yip
  - Ed Hollinger
  - James Pittman
  - Kelley Hitchman
  - Maryjane Farr
- **HRSA Representatives**
  - Adriana Martinez
  - Adriane Burton
  - Adrienne Goodrich-Doctor
  - Arjun Naik
  - Chris McLaughlin
  - Cliff Myers
  - Demonique (Nick) Lewis
  - Satish Gorrela
  - Vanessa Arriola
  - Vinay Vuyyuru
- **UNOS Staff**
  - Alex Tulchinsky
  - Amy Putnam
  - Anna Messmer
  - Bonnie Felice
  - Janis Rosenberg
  - Jason Livingston
  - Jerry DeSanto
  - Kristine Althaus
  - Liz Robbins Callahan
  - Lloyd Board
  - Marty Crenlon
  - Michael Ghaffari
  - Mike Ferguson
  - Morgan Jupe
  - Rebecca Murdock
  - Rob McTier
  - Roger Vacovsky
  - Susie Sprinson
  - Tiwan Nicolson