OPTN ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK Meeting Summary

OPTN Network Operations Oversight Committee
Meeting Summary
October 20th, 2022
Webex

Edward Hollinger, MD, PhD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 10/20/2022 to discuss the following agenda items:

1. Welcome
2. Member Institution Ransomware Incident
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 NOOC, provided an overview of the agenda.

2. Member Institution Ransomware Incident

Terri Helfrich, UNOS Director of Information Security, presented on a ransomware incident that happened at a member institution. The incident was reported to the OPTN Customer Service on October 12th and the OPTN IT Department was then notified immediately of the incident. The incident took place on October 2nd and the member institution reported the incident on October 12th. The transplant hospital was unaware of the expectation to notify UNOS in the event of an incident. It was noted that the OPTN could expand communications and education to raise awareness on what to do in these situations.

Summary of Discussion:

Committee Chair, Dr. Hollinger, opened the discussion portion, asking if there were steps that the OPTN could take to allow for earlier identification rather than depending on a member institution to notify the OPTN of an incident. Dr. Hollinger supported proactively reaching out to member institutions on what the OPTN can do to help when something like this occurs. This can reassure member institutions that the OPTN can provide support, while also allowing the OPTN to be aware of the situation. HRSA commented that many of the suggestions that were mentioned are factors that the NOOC is going to need to consider for the OPTN Security Framework. HRSA thought it was important for the NOOC to understand that the OPTN Contractor has a requirement for the NOOC to work with the OPTN to develop this framework, based on a new contract modification from HRSA.

A committee member asked if these expectations are going to be incorporated in OPTN bylaws or policies. UNOS staff responded yes, and that this was going to be discussed in more detail in the next section of the meeting.

A committee advisor commented that it would be valuable to provide members with templates of what an incident response plan must have to maintain access the OPTN Computer System. The template could include simple guidance and tools, as well as details on impacts to system access. The advisor noted that the OPTN does not want these incidents to disrupt transplantation, so having a response plan in place could help to minimize disruptions. He emphasized that organizations, especially smaller organizations, need these kinds of tools to help them create a response plan.

3. OPTN Member Information Security Policy and Bylaw Enhancements

Alex Tulchinsky, UNOS Chief Technology Officer, presented the new OPTN contract requirements that were assigned by HRSA to the OPTN Contractor. Liz Robbins Callahan, UNOS Special Counsel, explained that HRSA recently modified the contract to insert additional requirements related to IT. Some of the new requirements could be incorporated into the bylaw enhancement project that the NOOC is currently working on. It was noted that the NOOC has been discussing a lot of the requirements, but it is important that all the details and new requirements are presented to the NOOC, so they are aware of the scope of the contract modification. The requirements that the committee will be focusing on during the policy and bylaw enhancement were highlighted for the NOOC's awareness.

Rebecca Murdock, UNOS Policy Development Lead, introduced herself as the point of contact that has been brought in to help develop relevant policy language for the enhancement project. The main topics from the contract modification that the project needs to address are outlined as a framework for the committee to keep in mind. The group will be asked to reach consensus on multiple items so Ms. Murdock can format the committee's decisions into sound policy language. The committee will be asked to address the topics of security framework, access to the system, training, audit and compliance, and incident response management.

Terri Helfrich continued the conversation by recounting the survey that the committee was asked to complete, detailing the IT security frameworks of their institutions and the OPTN member type they represent. The committee was asked what kind of framework they would suggest adopting in the policy. The three options the committee considered was to adopt one framework for all OPTN members, adopting a framework specific to each member type, or allowing OPTN members to adopt any framework that meets certain security requirements.

After the presentation and discussion on the frameworks were completed, the committee was briefed on the other topics they needed to consider when approaching the project. For example, UNOS staff detailed the question of access control, awareness and training, audit and accountability, and incident response management.

Summary of Discussion:

A committee member noted that from an OPO perspective, he thinks that the OPTN would want one standard used for all OPTN member organizations. Another board member asked if there were any downsides to presenting one standard to all OPTN members. UNOS staff answered that they did not foresee any downsides, but the question was whether some members need the level of security that some other members do. The level of risk each member organization experiences could affect the kind of framework they may need. Thus, there is not a downside other than implementing a framework that may be more than an organization needs for their security purposes. A committee advisor asks what this policy is trying to protect and what the level of risk is, because this will affect what security standard they choose to apply. They noted that these systems are very complex and applying these standards will take a lot of work and energy on member's part.

Dr. Hollinger agreed with the committee advisor that the committee needs to get an assessment of the threat and the risk that each member type experiences. The level of maturity for different member organizations varies and that this should be accounted for when discussing their security needs. Dr. Hollinger expressed his concerns with a one framework fits all model, that this would be challenging for members because their systems are all very different from one another. For institutions that already have sound frameworks in place for their security systems, perhaps the OPTN could highlight certain areas they could improve their system and provide education on how to notify the OPTN when a security incident takes place. Conversely, if there are institutions that do not have frameworks in place, guiding them to a framework that has worked well for other similar institutions.

A committee advisor commented that there are multiple different levels of security that different member institutions could contain and there are different levels of risk associated with them. Their suggestion is assessing the risk of the different systems, and then analyzing the parameters for member institutions. Looking at the risk level may be more productive and make more sense than looking at different frameworks institutions could follow. This way, institutions are given what their system needs to protect and what their system should contain. UNOS staff sought clarity on what the committee believes is the OPTN's responsibility and what is the member institution's responsibility.

A committee member mentioned the difficulty they foresee in requiring a security measure in transplant centers because most transplant centers are a part of a much larger hospital. If a member institution has a framework that is deemed not to meet the standards, need to have it clearly laid out for them why their system is inadequate and what they can do to upgrade their system. This approach could appear more collegial than punitive to member institutions.

HRSA staff commented that the HRSA Administrator wants the OPTN to build a broader scope and to consider the risk of compromising patient data if the OPTN Computer System were to be compromised. The HRSA Administrator believes that is the OPTN's responsibility to figure out how to minimize these kinds of incidents from occurring. A committee member commented on the need for dialogue between the OPTN and member institutions if they are outside of the proposed framework requirements. The OPTN should learn how to work with these members to bring their systems up to an agreed upon standard, rather than limit access. HRSA commented that there should be an assessment on whether members are meeting the requirements of the system. There should be a framework in place, but also a routine assessment to ensure that members are adhering to the requirements. UNOS staff agreed that there should be a timeline that institutions are provided on how long they have to be compliant.

The committee chair commented on the fact that a lot of this project is going to be about the policies and details that the OPTN wants institutions to follow. He continued that more institutions have a robust IT system in place, but it is a question of whether or not these members have a framework in place that the OPTN deems acceptable. The chair thinks that making sure these details are laid out is going to be more complicated than the framework question and the OPTN should provide these institutions with guidance documents.

A committee advisor suggested that we use the systems that members have in place now and build their systems up from there, noting that it would be more difficult to start from scratch than to start with the systems that these institutions are already working with. They also comment that this project is going to be resource intensive.

A committee advisor asked the committee to consider any unintended consequences they could face if this framework is not fully vetted. HRSA staff noted that the committee should keep a system perspective during their work, and what needs to be put into place is a system with adequate security for people to have access to the OPTN Computer System. HRSA stated that the impact of the contractor is irrelevant, noting that the capacity of the contractor is for HRSA to worry about, not the committee.

Conversation from members in the meeting chat supported the option of allowing OPTN members to adopt any framework that meets certain security requirements. The Committee Chair agreed and thought that the other two frameworks would be nearly impossible for transplant centers to adopt for their entire centers, commenting that transplant programs are a small unit within bigger hospitals so it would be extremely difficult to have one uniform system for these members. He worried that if the committee went with any other framework other than this, that hospitals may start to opt out of having transplant units because it would be such a significant burden. He suggested that the committee figure out what pieces of the desired framework are important to maintain the integrity of the system, not the entire hospital system. A committee member agreed with Dr. Hollinger that this would be enormously difficult, especially for transplant hospitals because transplant is such a small portion of hospital's work. If the committee chooses to move towards a framework that needs more monitoring, then there is going to be a need for more employees. A committee advisor thought that bringing in a third-party auditors would be a great idea.

It was asked if there is a standard that hospitals follow for their security purposes and suggested looking at these frameworks because they assume that HRSA would accept these parameters. Another advisor expressed that although hospitals do have a standard in place, OPOs are excluded from these parameters, noting that there was a standard that was applied to hospitals and health systems but not OPOs. UNOS staff noted that an institutions maturity level is also important to consider, not only member type. A committee member asked how many histocompatibility labs are part of a health system, because they would assume that those labs already have adequate security because they would be part of a hospital based security. They note that OPOs are going to be the harder part of the security process. UNOS staff asked if the committee would like to focus on differences in member types and also consider institution size.

The committee chair noted it might be best to set a minimum framework and any framework that meets those requirements, is adequate. He suggested that the committee start by creating a list of requirements for organizations to evaluate their systems against. He also suggests continuously updating these requirements as systems change overtime. UNOS staff asked the committee what minimum requirements should be included in the enhancement project, noting that these requirements could be a list that the committee maintains and routinely updates.

During the discussion on access control, a committee member asked if there were ways for the OPTN to check member compliance. They asked if members are reviewing their systems on a quarterly basis or whether there is a guideline they must follow. UNOS staff explained that there has been discussion about site security administrators and how compliance would be checked.

NEXT STEPS:

The committee was asked to review the other topics that are relevant for them to consider and to bring back their ideas. The committee is asked to provide their feedback from the slides within the next two weeks so their feedback is incorporated into the enhancements draft that the committee will review next meeting.

Upcoming Meetings:

- November 15th, 2022

Attendance

- **Committee Members**
  - Bruno Mastroianni
  - Clifford Miles
  - Daniel Yip
  - Edward Hollinger
  - James Pittman
  - Kelley Hitchman
  - Kim Rallis
  - Melissa McQueen
- **HRSA Representatives**
  - Adrienne Goodrich-Doctor
  - Christopher McLaughlin
  - Clifford Myers
  - Nick Lewis
  - Satish Gorrela
- **UNOS Staff**
  - Alex Tulchinsky
  - Amy Putnam
  - Anna Wall
  - Bonnie Felice
  - Bridgette Huff
  - David Klassen
  - Bonnie Felice
  - Jason Livingston
  - Liz Robbins Callahan
  - Marty Crenlon
  - Mary Beth Murphy
  - Maureen McBride
  - Michael Ferguson
  - Michael Ghaffari
  - Morgan Jupe
  - Rebecca Murdock
  - Rob McTier
  - Roger Vacovsky
  - Sarah Payamps
  - Susie Sprinson
  - Terri Helfrich
  - Tiwan Nicholson
  - Tynisha Smith