OPTN ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK Meeting Summary

OPTN Transplant Administrator Committee
Fiscal Impact Advisory Workgroup
Meeting Summary
November 29, 2022
Conference Call

Susan Zylicz, Chair
Jason Huff, Vice Chair

Introduction

The Fiscal Impact Advisory Workgroup of the Transplant Administrator Committee met via Citrix GoToMeeting teleconference on 11/29/2022 to discuss the potential fiscal impact of the following public comment proposal on the OPTN histocompatibility laboratories (lab), organ procurement organizations (OPO), and transplant programs:

1. OPTN Member Information Security Policy and Bylaw Enhancements (Network Operations Oversight Committee)

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

1. OPTN Member Information Security Policy and Bylaw Enhancements

Overview of Proposal

The purpose of this proposal is to establish OPTN information security requirements for members to access the OPTN Computer System. The OPTN Network Operations Oversight Committee (NOOC) has developed the following draft recommendations to ensure network security:

- Require members to follow OPTN Contractor's term of use when using the OPTN Computer System
- Clarify which membership type includes access to the OPTN Computer System
- Define baseline security requirements for all OPTN members
- Require notice to the OPTN if an incident occurs at an OPTN member's institution that accesses the OPTN Computer System or with software exchanges data with the OPTN Computer System
  - Examples include ransomware attacks on electronic medical records and data leakage

The NOOC member noted several challenges to adopting enhanced OPTN security policies. These include the following:

- Not all member are Health Insurance Portability and Accountability Act (HIPAA) covered entities
- Consistent monitoring, administration, and compliance plan
  - OPTN Member Self-reporting through attestation
  - Audit every 3 years by OPTN selected 3rd party auditor
  - Report to OPTN within an hour of security incident at OPTN Member institution
- Consequences of violating security policies
  - Authority to deactivate system access for an entire OPTN Member institution
  - Notice and timing
  - Process for reactivation

The NOOC member added that the next step is to define baseline security requirements for all OPTN members and non-members. Non-members include contractors such as organ offer screening services.

Another NOOC member added that the cost might vary based on the type of requirement. For example, there might be a low impact on organizations to access the system by establishing user accounts and participating in security training. Other requirements that heighten the sense of security to ensure protection from malware and other threats might require additional costs. He further added that additional costs might be incurred by organizations if there is a security breach. This might include both a monetary impact as well as the inability to send or receive organ offers. Lastly, the NOOC member noted that information security assessment costs could vary depending on the type and size of an organization. For example, paying a third party company to assess a small organ procurement organization would cost approximately $40,000.

Workgroup Discussion

One member asked for clarification about application programming interface (API) compliance. The NOOC member explained that APIs are used to transfer data between computer systems. Compliance means that API systems are correctly installed and monitored for security. The intent is to increase the adoption of APIs to minimize duplicative data entry in order to improve data quality.

A member asked if the FIG was evaluating the fiscal impact of assessing member systems. One NOOC member responded that the cost is updating member security systems if needed, as well as the routine auditing costs. He added that security breaches could incur additional costs to members.

A member commented that it would be challenging to access the impact without knowing the minimum standards. He added that it might be possible to assess the incident process for a particular organization. However, if it is a stand-alone histocompatibility lab, they might not have standards to assess. He further added that larger institutions or healthcare systems would be less impacted while smaller organizations such as OPOs, and labs would be more impacted by the requirements.

A member noted that the OPO for her transplant center experienced a security breach, which hampered communication regarding organ offers. She added that lost opportunities for transplant are more than just financial costs and asked how those costs could be identified.

The NOOC member noted that identifying the required type of security framework could also affect costs. This could be a list of frameworks for members to use based on their individual needs. He added that this information might be identified during public comment and could impact smaller member organizations.

A member asked about assessing potential costs once security frameworks and thresholds are established. Staff noted the opportunity for the FIG to provide additional feedback following public comment.

A member expressed support for moving this forward, but noted the need for additional details before assessing the fiscal impact.

Next Steps

Staff will send the FIG survey to members following the call and draft the FIG analysis based on the responses. This information will then be shared with the NOOC.

Upcoming Meeting(s)

- TBD

Attendance

- **Fiscal Impact Advisory Workgroup Members**
  - Amber Carriker
  - Andrea Tietjen
  - Christopher Wood
  - Laura Stillion
  - John Gutowski
  - Kevin Koomalsingh
  - Jason Huff
  - Susan Zylicz
  - Stephanie Johnson
  - Lenore Hicks
- **HRSA Representatives**
  - Megan Hayden
- **SRTR Staff**
  - None
- **UNOS Staff**
  - Taylor Livelli
  - Robert Hunter
  - Kristina Hogan
  - Rebecca Murdock
  - Eric Messick
  - Morgan Jupe
  - Jerry Desanto
  - Kristine Althaus
  - Rob McTier
- **Other Attendees**
  - Cliff Miles
  - Bruno Mastroianni