The Transplant Institute METHODIST DALLAS **Methodist Dallas Medical Center**	**Title:** OPTN Cybersecurity Incident Reporting	**Effective Date:** 08/01/2023
	Section: Liver, Kidney and Pancreas	
Approved by: Alejandro Mejia, M.D., Executive Program Director Denise Harrington, VP Transplant Services Melody Holder, Director, Clinical Transplant Operations		**Revision Date(s):** 04/01/2025 **Next review Date:** 04/01/2028

Purpose:

To outline the process of reporting declared cybersecurity incidents surrounding the organ transplant program's computing environment as defined in the OPTN Policy 3.1.C

Policy:

The organ transplant program will follow the process outlined below to report declared cybersecurity incidents:

- If a transplant employee reasonably suspects that a cybersecurity incident has occurred or is occurring, the employee must report that to the Methodist Health System (MHS) IT help desk at 214-947-1999 (x 71999) according to **MHD IT 006: Security Incident Response Plan** policy. To comply with OPTN policy, the employee will also report that incident to the designated information security officer as outlined by OPTN.

- If a non-transplant employee identifies a cybersecurity incident across the system, the MHS Enterprise Security and Architecture (ESA) team will notify the designated information security officer.

- The designated information security contact will report declared cybersecurity incidents as defined in the policy notice to the OPTN. Once a cybersecurity incident has been identified within the scope of the policy notice, the information security contact must report this information to the Organ Center by calling at (800) 292-9537 within the following timeframes:

    - If in the cybersecurity incident, the member did NOT disconnect access to UNet for the affected user(s) and/or any impacted systems, this information must be reported to the OPTN within 24 hours following the information security contact becoming aware of the security incident.

    - If in the cybersecurity incident, the member DID disconnect access to UNet for the affected user(s) and/or any impacted systems, this information must be reported to the OPTN within 72 hours following the information security contact becoming aware of the security incident.

For the purposes of this policy, the designated information security contact will be the Director of Clinical Transplant Operations, Director of Business Operations or Transplant Senior Analyst as a back-up.