

Report in Brief

Date: August 2022

Report No. A-18-21-11400

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL



Why **OIG** Did This Audit

The Organ Procurement and Transplantation Network (OPTN) is part of the Health Resources and Services Administration (HRSA) national system that allocates and distributes donor organs to individuals waiting for an organ transplant. OPTN is a public-private partnership that links all professionals involved in the U.S. donation and transplantation system.

Our objective was to determine whether HRSA implemented selected cybersecurity controls over the OPTN to protect the confidentiality, integrity, and availability of transplant data, in accordance with Federal requirements.

How **OIG** Did This Audit

We reviewed a selected number of general information technology (IT) controls that the United Network for Organ Sharing (UNOS) had implemented for the OPTN and determined whether HRSA was providing adequate oversight to ensure the general IT controls were implemented in accordance with Federal requirements. To accomplish our objective, we requested and reviewed general IT controls documentation over OPTN provided by UNOS and HRSA for only the selected controls. In addition, we interviewed personnel from HRSA and UNOS and obtained demonstrations of those selected OPTN general IT controls.

The Health Resources and Services Administration Should Improve Its Oversight of the Cybersecurity of the Organ Procurement and Transplantation Network

What **OIG** Found

HRSA had ensured that most of the general IT controls that we selected to test were implemented for OPTN by UNOS to protect the confidentiality, integrity, and availability of transplant data in accordance with Federal requirements. However, we identified areas for which HRSA could improve its oversight of UNOS to ensure that all Federal cybersecurity requirements are being met in a timely manner. We noted that HRSA could improve its oversight of UNOS to ensure that UNOS performs adequate reviews of local user access of the OPTN, and that certain key cybersecurity policies and procedures were finalized and in place.

What **OIG** Recommends and HRSA's Comments

We recommend that HRSA develop additional oversight controls and procedures (e.g., deliverable schedules, compliance assessments, and monitoring) to ensure that the OPTN contractor complies with all Federal cybersecurity requirements and implements security controls over the OPTN in an effective and timely manner.

HRSA stated that it has made efforts to continuously strengthen its oversight and controls over OPTN. HRSA added a federal employee to serve as the OPTN Information System Security Officer to provide oversight of security controls, security procedures, security deliverable schedules, and security compliance assessments. In addition, HRSA indicated it has taken action to finalize the policies and procedures that were in draft during our audit and improve the access controls of OPTN.