Codify
BY AAPC

Health Information Compliance Alert

Industry Notes: OIG Homes In on Cybersecurity at Organ Procurement and Transplantation Network

As one of the nation's top enforcement agencies, the HHS Office of Inspector General (OIG) works to improve transparency and provide oversight across the spectrum of federal healthcare programs. In a recent report, the national watchdog shines a spotlight on emerging cyber threats to the Organ Procurement and Transplantation Network (OPTN).

Context: The OPTN, which falls under the umbrella of Health Resources and Services Administration (HRSA) and is a private/public partnership, connects all professionals across the country involved in the organ donation and transplant system. Due to the importance of the program, OIG decided to audit the cybersecurity controls of the OPTN to ensure the "confidentiality, integrity, and availability of transplant data" and to review alignment with federal requirements, a report indicates.

Overall, OIG found HRSA to be compliant, but that the agency could better supervise policies and IT implementation at United Network for Organ Sharing (UNOS).

"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," OIG says.

HRSA responded to OIG's report and offered that it had already addressed concerns with the following updates, according to the report:

- Tap a federal employee to act as an OPTN Information System Security Officer (ISSO) to provide oversight of security controls, security procedures, security deliverable schedules, and security compliance assessments.
- Move security policies and procedures from the documentation stage to implementation.
- Add multifactor authentication to the login regime.
- Beef up "offboarding" program for inactive accounts.

Read the report at https://oig.hhs.gov/oas/reports/region18/182111400.pdf.