Report in Brief
Date: September 2022
Report No. A-18-21-03100

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

The IHS Telehealth System Was Deployed Without Some Required Cybersecurity Controls

Why OIG Did This Audit

In response to the COVID-19 pandemic, health care providers increasingly deliver care using telehealth technologies. These technologies improve access to care, increase patient convenience, and increase service-delivery efficiency.

Our objective was to determine whether the Indian Health Service (IHS) implemented select cybersecurity controls to protect its telehealth system.

How OIG Did This Audit

We reviewed applicable IHS and HHS policies and procedures for telehealth technologies, interviewed staff, and reviewed system security documentation to determine whether IHS telehealth technologies was secure. We focused on determining whether IHS designed and implemented cybersecurity controls that are essential to securing IHS telehealth systems components before deployment.

What OIG Found

Although IHS deployed a national telehealth system, which increased the availability of health care services during the pandemic, it did not complete select IT controls as required prior to deploying its telehealth system nationally. Specifically, IHS did not complete the contingency plan, risk assessment, finalized authorization to operate (ATO), and system security plan. Additionally, after deployment of the telehealth system, IHS did not remediate known vulnerabilities on some telehealth system devices in a timely manner.

Controls were not implemented because, according to IHS officials, IHS did not have a strategy for completing the requirements to implement and authorize a new information system to operate in an expedited fashion to meet an urgent, mission-critical need. IHS has since completed the controls covered by this audit, and no major incidents or breeches have been reported to HHS. However, IHS assumed an undetermined level of risk to the security of the system and data by not ensuring that all required IT controls were in place to protect the system before deployment.

What OIG Recommends and IHS Response

We recommend that the Indian Health Service develop a strategy for identifying, implementing, and testing cybersecurity controls for new information systems that are deployed in an expedited fashion to meet an urgent, mission-critical need. The strategy should define the minimum set of critical controls that must be implemented and tested before the system is deployed, noting the acceptance of risk for not implementing all required controls and stipulate that the full ATO process will be completed within a specific time period. We also recommend that the Indian Health Service ensure that adequate policies, procedures, and training are implemented to ensure that known telehealth vulnerabilities are remediated in a timely manner.

IHS concurred with our recommendations and will develop guidance for inclusion in the IHS *Indian Health Manual* for expeditiously deploying a new information system for use during emergencies when it is necessary to meet an urgent, mission-critical need. In addition, IHS will review related policies, procedures, and training to ensure that they are adequate to address all known system vulnerabilities by December 31, 2022.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/182103100.asp.