Report in Brief
Date: July 2019
Report No. A-18-17-11400

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

IHS Needs To Improve Oversight of Its Hospitals' Opioid Prescribing and Dispensing Practices and Consider Centralizing Its Information Technology Functions

Why OIG Did This Review

Prescription opioids continue to contribute to the opioid overdose epidemic. A prior OIG audit identified high volumes of opioid purchases in IHS communities. In addition, the prior OIG audit of two IHS hospitals determined that IHS did not have adequate information technology (IT) security controls to protect health information and patient safety. The audit also found significant differences in the way the two hospitals carried out their respective IT operations.

We conducted this audit to analyze and compare opioid prescribing and dispensing practices and IT operations at five other IHS hospitals.

Our objectives were to determine whether (1) the hospitals we reviewed prescribed and dispensed opioids in accordance with IHS policies and procedures and (2) IHS's decentralized IT management structure affected its ability to deliver adequate IT and information security services at its hospitals in accordance with Federal requirements.

How OIG Did This Review

We reviewed IHS's opioid prescribing and dispensing practices and information system general controls at five IHS hospitals. In addition, we reviewed a judgmental sample of 150 patients' records. Also, we performed a penetration test at each hospital.

What OIG Found

The IHS hospitals we reviewed did not always follow the Indian Health Manual when prescribing and dispensing opioids. Specifically, through our patient record review, we found that hospitals did not always review the course of patient treatment and causes of pain within required timeframes, perform the required urine drug screenings within recommended time intervals, review patient health records before filling a prescription from a non-IHS provider, and maintain pain management documents to support that provider responsibilities had been performed. We also found that these IHS hospitals did not fully use the States' prescription drug monitoring programs when prescribing or dispensing opioids.

IHS's decentralized IT management structure led to vulnerabilities and weaknesses in implementing security controls at all five hospitals. IHS's controls were not effective at preventing or detecting our penetration test cyberattacks. In addition, the hospitals implemented IT security controls to protect health information and patient safety differently. Inconsistencies in the delivery of cybersecurity services can lead to the same vulnerability being remediated at one hospital but being exploited at another hospital that did not remediate the vulnerability. As a result, IHS hospital operations and delivery of patient care could have been significantly affected.

What OIG Recommends and IHS Comments

We recommend that IHS work with hospitals to ensure they follow the Indian Health Manual when prescribing and dispensing opioids. We also recommend that IHS consider centralizing its IT systems, services, and functions by conducting a cost-benefit analysis of adopting a cloud computing policy, including centralization of IT systems, services, and functions. We made other procedural recommendations, which are listed in the report. We provided more detailed information and specific recommendations to IHS so that it can address specific vulnerabilities that we identified.

In written comments to our draft report, IHS concurred with our recommendations and described actions it has taken or plans to take to address our findings.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181711400.asp.