Report in Brief
Date: February 2020
Report No. A-18-19-06003

U.S. Department of Health & Human Services
Office of Inspector General

Why We Did This Review

For fiscal year 2019, the Department of Health and Human Services (HHS), Office of Inspector General (OIG) received $5 million in congressional appropriations to conduct oversight of the National Institutes of Health (NIH) grant programs and operations. Among the issues of interest to Congress were matters pertaining to cybersecurity protections and NIH compliance with Federal requirements.

The Clinical Research Information System (CRIS) contains the Electronic Health Records (EHR) for patients of NIH's Clinical Center. The data and the IT security controls protecting the data are of significant importance to both HHS and the Federal government. OIG engaged CliftonLarsonAllen LLP (CLA) to conduct this audit.

The objective was to determine if the EHR System at NIH – also known as CRIS - has effective IT controls and to understand how NIH receives, processes, stores and transmits EHR records into CRIS.

How We Did This Review

To accomplish our objective, CLA reviewed NIH's policies and procedures; tested system security controls and configurations; and inspected public information on NIH's website. CLA also conducted interviews with NIH Clinical Center staff to determine how NIH ensures the integrity of EHR data as well as to document how NIH ingest EHR records.

National Institutes of Health Had Information Technology Control Weaknesses Surrounding Its Electronic Health Record System

What We Found

CLA found that NIH had certain controls in place to secure EHR information and information systems. However, NIH's information security policies and practices were not operating effectively to preserve the security, confidentiality, integrity, and availability of NIH's EHR information and information systems, resulting in potential risks of unauthorized access, use, disclosure, disruption, modification, or destruction. Specifically, (i) the primary and alternate processing sites were located adjacent to each other on the NIH campus and not geographically distinct; (ii) servers supporting the EHR were still in operation despite nearing end-of-life on extended support without an effective transition plan; and (iii) terminated users and inactive accounts were not deactivated in a timely manner.

These weaknesses existed because, at the time of the fieldwork, NIH located their alternate processing site in the same geographic location as their primary site; NIH delayed software upgrades until completion of system upgrades had been completed; and NIH had not yet fully implemented the automated tool that was intended to ensure users and inactive accounts were deactivated timely. CLA shared the preliminary findings with NIH in advance of issuing the draft report. Before issuing the draft report, NIH implemented some of the recommendations.

What We Recommend and NIH Comments

CLA recommends that NIH Clinical Center Management (1) Complete the NIST requirements for implementing an alternative processing site that is a reasonable and viable option. Identify, document, and implement actions to mitigate risks of using existing alternative site based on the risk assessment results until compliant alternate site is established; (2) implement policies and procedures to ensure all software is upgraded or replaced prior to end of life; and (3) ensure that the automated CRIS User Account Management tool is operating so that all changes to user privileges are authorized, properly documented, and inactive accounts are deactivated.

In written comments to the draft report, NIH concurred with all of the recommendations and described actions it has taken or plans to take to address the findings.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181906003.