Audit Highlights

Highlights of performance audit report on the Division of Health Care Financing and Policy, Information Security issued on March 22, 2022.

Legislative Auditor report # LA22-12.

Background

The mission of the Division of Health Care Financing and Policy (Division) is to: 1) purchase and provide quality health care services to low-income Nevadans in the most efficient manner, 2) promote equal access to health care at an affordable cost to the taxpayers of Nevada, 3) restrain the growth of health care costs, and 4) review Medicaid and other state health care programs to maximize potential federal revenue. The Division administers both Nevada Medicaid and Check Up programs.

The Medicaid Management Information System (MMIS) is a computerized claims processing and information retrieval system the Nevada Medicaid program must have to be eligible for federal funding.

In fiscal year 2021, the Division was primarily funded with federal grants totaling $3.7 billion and state appropriations of about $873 million. As of June 2021, the Division had 261 filled positions located in its Carson City, Elko, Las Vegas, and Reno offices. Eighteen of these positions are dedicated to information technology (IT) activities. One position leads the Business Process Management Unit; three support the Information Security Office; six support the Project Management Office; and eight provide support for the Division's systems, network, and help desk.

Purpose of Audit

The purpose of the audit was to determine if the Division of Health Care Financing and Policy has adequate controls to ensure user access controls protect its sensitive information and to monitor its MMIS change management process. The audit included the systems and practices in place during fiscal year 2021, and fiscal year 2020 for enhancement projects.

Audit Recommendations

This audit report includes six recommendations to improve information security access controls to users of the Medicaid Management Information System.

The Division accepted the six recommendations.

Recommendation Status

The Division's 60-day plan for corrective action is due on June 15, 2022. In addition, the 6-month report on the status of audit recommendations is due on December 15, 2022.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

Information Security

Division of Health Care Financing and Policy

Summary

The background investigation process at the Division can be strengthened. Specifically, non-Division state employees and Division IT contractors were given access to the Medicaid Management Information System without verifying or documenting a background check was completed. In addition, some fiscal agent employees' user accounts were enabled before the Division received background investigation information and authorized access. Finally, newly hired Division employees did not receive a preliminary background investigation or submit their background investigation packet before they were given access to MMIS. Background investigations help reduce the risk sensitive data will be accessed by disreputable individuals.

The Division does not actively manage MMIS user accounts. Specifically, the Division does not ensure MMIS access is still needed for non-Division state employees. In addition, the Division does not ensure that user accounts of former state employees and its fiscal agent are disabled timely. Finally, the Division does not ensure documentation used to authorize user MMIS access is complete or reviewed periodically. Accounts still valid after a user leaves an enterprise make it easier for an external or internal threat actor to gain unauthorized access to enterprise data using valid user credentials.

Key Findings

The Division did not verify or document background investigations were performed for non-Division state employees and Division IT contractors that were granted access to MMIS. For 84 non-Division employees, the Division did not verify background checks were performed. In addition, we randomly selected 7 of the Division's 13 IT contractors for testing. For four of seven (57%) contractors tested, the Division had no record a background investigation was conducted. (page 3)

Fiscal agent staff were given MMIS access before proper authorization. We identified 2 of 10 (20%) fiscal agent user accounts that were enabled in the system prior to the background investigation process being initiated and authorized by the Division. (page 4)

For all newly hired Division employees in fiscal year 2021, access was granted to MMIS prior to completing a preliminary or fingerprint background investigation. A preliminary background investigation consists of a national records check that provides detailed background information based on someone's name and Social Security number and can be performed before a more thorough fingerprint background check. (page 5)

The Division does not have a process to actively manage non-Division state employee user accounts and ensure system access is still needed. For 11 of 79 (14%) non-Division state employee MMIS user accounts tested, the employee had never logged into MMIS since being given access. Three accounts have remained enabled for over 2 years without any login activity. In addition, nine other employees have not logged into MMIS since before June 2021. One employee has not logged into the system for over 2.5 years. Instead of actively managing user accounts, the Division relies on other state agencies and the fiscal agent to notify them when access is no longer needed. (page 7)

During our testing of user accounts, we identified four non-Division state employees that ended state employment before June 30, 2021, while their user accounts remained active for months after they terminated employment with the State. In addition to state employees, we tested accounts of all seven fiscal agent users who were identified as terminated. One account was disabled the same day of termination while six remained enabled for several days to several months. (page 7)

The Division did not properly document system access authorization or documentation was inaccurate on the MMIS security access request forms. For 23 non-fiscal agent system access forms tested, we observed for some forms supervisor or information security officer approval was not documented, user roles were not documented, or approved user roles did not agree to user roles assigned in the system. In addition, the Division could not provide system access request forms for three users. (page 9)

The Division's MMIS enhancement process is effective in ensuring changes to the system are prioritized and completed. A documented change management plan is utilized and monitored. In addition, the Division monitors hours charged to individual projects. Proper management of this process helps ensure changes to the MMIS meet the needs of stakeholders and align with available resources. (page 11)

Audit Division
Legislative Counsel Bureau