Audit Highlights

Highlights of performance audit report on the Silver State Health Insurance Exchange, Information Security issued on September 10, 2024.

Legislative Auditor report # LA24-14.

Background

The Silver State Health Insurance Exchange (Exchange) is the state agency that operates the online marketplace known as Nevada Health Link where eligible Nevada consumers can shop for, compare, and purchase quality and affordable health insurance plans. The Exchange facilitates and connects eligible Nevadans who are not insured by their employer, Medicaid, or Medicare to health insurance options. Individuals can purchase Affordable Care Act certified qualified health plans through the state-based exchange platform and, if eligible, can receive subsidy assistance to help offset their monthly premiums and out-of-pocket costs.

Established in 2011, the Exchange was created to function as a state-based health insurance exchange. However, from calendar year 2015 to the beginning of 2019, the Exchange utilized a federal platform called HealthCare.gov for the enrollment of Nevada residents. At the end of 2019, the Exchange transitioned to a state-based marketplace, NevadaHealthLink.com. The Exchange has contracted the enrollment, eligibility, and call center functions of the state-based exchange platform to a contractor.

Purpose of Audit

The purpose of the audit was to determine if the Exchange has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems. Our audit focused on the systems and practices in place during fiscal years 2023 and 2024.

Audit Recommendations

This audit report contains 11 recommendations to improve information security controls of the Exchange's systems.

The Exchange accepted the 11 recommendations.

Recommendation Status

The Exchange's 60-day plan for corrective action is due on December 9, 2024. In addition, the 6-month report on the status of audit recommendations is due on June 9, 2025.

Information Security

Silver State Health Insurance Exchange

Summary

Improvements can be made to enhance information security controls meant to protect the confidentiality, integrity, and availability of the Exchange's systems. The Exchange's user access requests, authorizations, and monitoring practices were incomplete and undocumented. In addition, the Exchange does not verify that all users with access to the state-based exchange platform have completed a pre-access background check before granting system access. Furthermore, signed user access agreements have not been properly maintained or documented for all state-based exchange platform users. The Exchange's mandatory quarterly user access reviews have not been documented. In addition, security awareness training procedures and training policies have not been created or implemented. Finally, multiple users with state-based exchange platform access had not completed the assigned security awareness training, and the process to ensure completion was not effective.

The Exchange's key information security processes can be strengthened. In addition, the asset inventory process used at the Exchange needs to be further developed. Finally, the process for ensuring local administrator accounts are disabled needs to be implemented. Inadequate information security processes increase the risk of data loss, productivity loss, noncompliance, and reputational damage.

Our review of physical and environmental security controls concluded the Exchange can improve its key control process which includes physical and digital keycard management. Further, while the Exchange has a server room containing limited essential equipment and requires keycard access, the server room door provides minimal physical security. Physical security controls have a direct impact on the Exchange's ability to mitigate loss, disclosure, or inappropriate use of assets and protected data.

Key Findings

While we noted various opportunities for improvement, our work did not identify any critical security vulnerabilities at the Exchange within our testing areas. (page 4)

The Exchange's user access request practices lack consistency and documentation across the various user types accessing the state-based exchange platform. For 29 of the 30 users tested, the Exchange was unable to produce evidence of access request forms or other records of access approval. (page 4)

The Exchange's process for ensuring background checks are completed does not verify all users receive them. For the 30 users tested, the Exchange was unable to produce evidence it verified that a background check had been completed before granting or allowing access to the state-based exchange platform. (page 5)

The Exchange does not have a process in place to ensure all users accessing the state-based exchange platform, which contains Nevada citizens' personally identifiable information have read and signed the required acceptable use agreement. For the 30 state-based exchange platform users tested, the Exchange was unable to produce any documentation of a signed acceptable use agreement. (page 6)

The Exchange does not have any documentation to verify that quarterly user access reviews are being conducted. Exchange management explained to the auditors that a quarterly review is occurring; however, the review has never been documented and there is no formal process to perform or document quarterly reviews. (page 7)

Better oversight of the Exchange's security awareness training program for employees and contractors is needed. We identified 22 of 30 users tested did not complete their annual refresher security awareness training, or the Exchange was unable to produce evidence of its completion. (page 7)

The risk management process can be further developed to include an assessment of internal information technology (IT) systems. During discussions with management, it was confirmed that no risk assessment is completed for IT on the local Exchange network including servers and workstations. (page 9)

The Exchange's asset inventory practices are weak and need improvement as they relate to computer hardware used by the agency. After reviewing different reports of the Exchange's computer hardware assets, we observed significant discrepancies in physical inventory reconciliation. (page 10)

The Exchange does not adequately manage digital keycards and physical key access. While the Exchange utilizes the state's keycard access system, keycard accounts were not reviewed regularly to ensure the continued need for access to secure areas. (page 12)

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

Audit Division
Legislative Counsel Bureau