Report in Brief

Date: November 2018
Report No. A-18-17-09302

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

Why OIG Did This Review

The HHS OIG's reviews of information system general controls at two Medicaid managed care organizations (MCOs) in Arizona identified numerous security vulnerabilities. The Arizona Health Care Cost Containment System administers Arizona's Medicaid program and is the State agency responsible for monitoring the operations of its contracted MCOs. The MCOs' systems depend on the effectiveness of information system general controls, which are critical to the confidentiality, integrity, and availability of Medicaid data.

Our objective for this review was to summarize the security vulnerabilities that we identified as audit findings in our reviews of whether the two Arizona Medicaid MCOs adequately protected their Medicaid managed care data and information systems in accordance with the Health Insurance Portability and Accountability Act (HIPAA) guidelines.

How OIG Did This Review

We summarized the security vulnerabilities from our reviews into two core categories of general controls—access controls and configuration management.

Summary of Security Vulnerabilities Identified at Two Arizona Managed Care Organizations and Inconsistent Treatment of Medicaid Data Security at the State Agency and Managed Care Organizations

What OIG Found

This summary report consolidates the findings from our two individual reports while omitting details that could compromise the security of any specific MCO that we audited. Our consolidated findings from the reviews of the MCOs show significant vulnerabilities in the MCOs' information systems, and raise concerns about the integrity of the systems used to process Medicaid managed care claims. Some of the same vulnerabilities were identified at both MCOs, suggesting that other Arizona MCO information systems may be similarly vulnerable. Additionally, existing Federal regulations treat the security of Medicaid data differently depending on whether the data reside at the State agencies or at the MCOs. This disparate application of security requirements for Medicaid data could affect State-MCO relationships nationwide and could increase risk to Medicaid patient data.

What OIG Recommends and CMS Comments

We recommend that CMS: 1) conduct a documented risk assessment and determine how the disparate application of Federal security requirements impacts cybersecurity risk for Medicaid data maintained by MCOs and what actions should be taken to address any oversight gap; and 2) inform all State agencies of the types of vulnerabilities we identified at the Arizona MCOs to enhance nation-wide awareness of cybersecurity weaknesses.

CMS did not concur with our recommendation to conduct a documented risk assessment but did concur with our recommendation to inform all State agencies of the cybersecurity vulnerabilities we identified at the Arizona MCOs. CMS stated that the Medicaid managed care regulations help ensure the security of beneficiaries' data and CMS believes that it is clear that the phrase stated within the regulations "any other applicable Federal and state laws" would require MCOs, under contract with a State, to fully comply with HIPAA security requirements. In addition, CMS stated that a risk assessment is already a requirement under the jurisdiction of the HHS Office for Civil Rights (OCR) and it would be duplicative of existing risk assessment efforts.

Since this issue resides in the Medicaid program and OCR is not responsible for the disparate application of Federal security requirements, OIG believes that CMS is in the best position to ensure that data security regulations are consistently applied to protect Medicaid beneficiaries' data, regardless of where the data resides.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181709302.asp.