

Report in Brief

Date: August 2017

Report No. A-07-16-00469

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



Why OIG Did This Review

The U.S. Department of HHS oversees States' administration of various Federal programs, including Medicaid. State agencies are required to establish appropriate computer system security requirements and conduct biennial reviews of computer system security used in the administration of State plans for Medicaid and other Federal entitlement benefits. This review is one of a number of HHS OIG reviews of States' computer systems used to administer HHS-funded programs.

Our objective was to determine whether the North Carolina State Medicaid agency (State agency) had implemented adequate information system general controls over the North Carolina Medicaid claims processing systems in accordance with Federal requirements.

How OIG Did This Review

The State agency contracts with CSRA, Inc., to operate North Carolina's Medicaid claims processing systems. We assessed the effectiveness of the information system general controls over computer operations at CSRA as those controls related to the North Carolina Medicaid program claims processing for State fiscal year 2016. We reviewed CSRA's information system general controls relating to entity-wide security, access controls, configuration management, network device management, service continuity, mainframe operations, and application change control.

Public Summary Report: The State of North Carolina Did Not Ensure That Federal Information System Security Requirements Were Met for Safeguarding Its Medicaid Claims Processing Systems and Data

What OIG Found

The State agency had not ensured that CSRA implemented adequate information system general controls over the North Carolina Medicaid claims processing systems in accordance with Federal requirements. The vulnerabilities that we identified increased the risk to the confidentiality, integrity, and availability of North Carolina's Medicaid data.

Although we did not identify evidence that the vulnerabilities had been exploited, exploitation could result in unauthorized access to and disclosure of sensitive information, as well as disruption of critical North Carolina Medicaid operations. As a result, the vulnerabilities are collectively and, in some cases, individually significant and could potentially compromise the confidentiality, integrity, or availability of North Carolina's Medicaid claims processing data and systems. In addition, without proper safeguards, systems are not protected from individuals and groups with malicious intent to obtain access in order to commit fraud or abuse or launch attacks against other computer systems and networks.

What OIG Recommends and State Agency Comments

We recommend that the State agency improve the protection of sensitive data on its Medicaid claims processing systems by working with CSRA to address the vulnerabilities identified during our audit to ensure compliance with Federal requirements.

The State agency concurred with our recommendations and described corrective actions that it had taken or planned to take.