Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PUBLIC SUMMARY REPORT: VIRGINIA DID NOT ADEQUATELY SECURE ITS MEDICAID DATA

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

May 2017
A-04-15-05066

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Virginia did not adequately secure its Medicaid data and information systems, which potentially compromised the integrity of its Medicaid program and could have resulted in unauthorized access to and disclosure of Medicaid beneficiary information.

This summary report provides an overview of the results of our audit of the information system general controls over the Virginia Medicaid claims processing systems. It does not include specific details of the vulnerabilities that we identified because of the sensitive nature of the information. We have provided more detailed information and recommendations to the Virginia Department of Medical Assistance Services (DMAS) so that it can address the issues we identified. The findings listed in this summary report reflect a point in time regarding system security and may have changed since we reviewed these systems.

WHY WE DID THIS REVIEW

The U.S. Department of Health and Human Services (HHS) oversees States' use 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 (45 CFR § 95.621). This review is one of a number of HHS, Office of Inspector General, reviews of States' computer systems used to administer HHS-funded programs.

DMAS is the single Virginia agency designated to administer or supervise the administration of Virginia's Medicaid program. In administering this program, DMAS uses an outside contractor to develop and operate the Virginia Medicaid claims processing system. Virginia's Medicaid program processed $8.2 billion in claims for 1,277,214 beneficiaries in fiscal year (FY) 2015. The Virginia Information Technology Agency (VITA) supports the DMAS Medicaid Management Information System[1] (MMIS) by providing cybersecurity, information technology (IT) infrastructure services, and IT governance. VITA uses the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, as its security standard and requires its use throughout Virginia.

The objective of our audit was to determine whether Virginia adequately secured its Medicaid data and information systems in accordance with Federal requirements.

HOW WE CONDUCTED THIS REVIEW

We assessed Virginia's policies, procedures, and information system general controls over its MMIS in place as of September 2015. To accomplish our objective, we reviewed Virginia's information system general controls over its computer-processed data using MMIS security

[1] Sections 1903(a)(3) and 1903(r) of Title XIX of the Social Security Act require States to implement an MMIS to enhance the efficiency and effectiveness of the Medicaid program. MMIS is a commonly accepted term for an automated claim processing and information retrieval system used to process Medicaid claims and to produce service utilization and management information required for program administration and audit purposes.

requirements[2] and related NIST security control guidance. We reviewed Virginia's MMIS policies and procedures, interviewed staff, and reviewed supporting documentation provided by Virginia. In addition, we used vulnerability assessment scanning software to determine whether security-related vulnerabilities existed on selected network devices, Web sites, servers, and databases supporting the MMIS.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We communicated to Virginia our preliminary findings in advance of issuing our draft report.

WHAT WE FOUND

Virginia did not adequately secure its Medicaid data and information systems in accordance with Federal requirements. Although Virginia had adopted a security program for its MMIS, numerous significant system vulnerabilities remained. These vulnerabilities remained because Virginia neither implemented sufficient controls over its Medicaid data and information systems nor provided sufficient oversight to ensure that its contractor implemented contract security requirements. Although we did not identify evidence that anyone had exploited these vulnerabilities, exploitation could have resulted in unauthorized access to and disclosure of Medicaid beneficiary data, as well as the disruption of critical Medicaid operations. These vulnerabilities were collectively and, in some cases, individually significant and could have compromised the integrity of Virginia's Medicaid program.

WHAT WE RECOMMENDED

We recommended that Virginia improve its Medicaid security program to secure Medicaid data and information systems in accordance with Federal requirements, provide adequate oversight to its contractor, and address the vulnerabilities identified during our audit. Specifically, we recommended that Virginia enhance its Medicaid:

- systems and information integrity controls,
- risk management process,
- access and authentication controls,
- audit and accountability controls,
- system and communications protection controls, and

[2] We did not review the MMIS information system requirements for physical security, contingency plans, emergency preparedness, or designation of an information system security manager.

- configuration management controls.

VIRGINIA COMMENTS

In written comments on our draft report, Virginia concurred with our recommendations and described corrective actions that it had taken or planned to take.

APPENDIX: RELATED OFFICE OF INSPECTOR GENERAL REPORTS

AUDITS OF MEDICAID MANAGEMENT INFORMATION SYSTEM AT STATES

Report Title	Report Number	Date Issued
Public Summary Report: Information Technology Control Weaknesses Found at the Commonwealth of Massachusetts' Medicaid Management Information System	A-06-15-00057	3/2017
Public Summary Report: The State of Colorado Did Not Meet Federal Information System Security Requirements for Safeguarding Its Medicaid Systems and Data	A-07-15-00463	10/2016
Public Summary Report: South Carolina Did Not Meet Federal Information System Security Requirements for Safeguarding Medicaid Management Information System Data and Supporting Systems	A-04-13-05049	2/2016