Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PUBLIC SUMMARY REPORT: SOUTH CAROLINA DID NOT MEET FEDERAL INFORMATION SYSTEM SECURITY REQUIREMENTS FOR SAFEGUARDING MEDICAID MANAGEMENT INFORMATION SYSTEM DATA AND SUPPORTING SYSTEMS

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

Thomas M. Salmon
Assistant Inspector General
for Audit Services

February 2016
A-04-13-05049

Office of Inspector General

http://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.

South Carolina Department of Health and Human Services did not meet Federal information system security requirements for safeguarding Medicaid Management Information System data and supporting systems. The resulting security vulnerabilities increased the risk of unauthorized access to beneficiaries' electronic protected health information.

This summary report provides an overview of the results of our audit of the information security controls at the South Carolina (State) Medicaid Management Information System (MMIS). 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 State so that it can address the issues we identified. The findings listed in this summary reflect a point in time regarding system security and may have changed since we reviewed these systems.

WHY WE DID THIS REVIEW

We selected the State MMIS for review because of reported data breaches of State information systems and the age of its MMIS. The State had two significant data breaches in 2012: the theft of 228,435 Medicaid electronic records from the State's Department of Health and Human Services and the theft of approximately 74 gigabytes of social security and credit card information from the State's Department of Revenue. Also, during a January 2013 meeting with the Centers for Medicare & Medicaid Services (CMS) Consortium for Medicaid and Children's Health Operations, CMS officials expressed concerns about the State's MMIS infrastructure because its systems were more than 30 years old.

The State's Department of Health and Human Services is responsible for administering the State Medicaid program. The State is its own fiscal agent that houses, supports, provides IT services, and provides operational support for its MMIS and the Medicaid Eligibility Determination System through a contract with Clemson University (Contractor). The State Medicaid program processed $5 billion in claims for 966,602 beneficiaries in calendar year 2012.

Our objective was to determine whether the State safeguarded MMIS data and supporting systems in accordance with Federal requirements.

HOW WE CONDUCTED THIS REVIEW

We reviewed the State's MMIS controls in place as of March 2013, which included reviewing applicable policies and procedures and interviewing the State and Contractor personnel responsible for the implementation and security of the State's MMIS. We also reviewed the State's system security plan and risk assessment of the information system and information that it processes, stores, or transmits; reviewed its process for identifying vulnerabilities; tested its patch management process for operating systems and software; tested software and data security controls; tested telecommunications security; and performed and reviewed vulnerability scans of certain Web applications and databases.

We did not evaluate the State's internal controls as a whole. We performed our fieldwork at the State's headquarters in Columbia, South Carolina, and at its Contractor's location in Anderson, South Carolina, from March to September 2013.

We conducted the performance audit described here 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 provided a reasonable basis for our findings and conclusions based on our audit objectives.

WHAT WE FOUND

The State had not safeguarded MMIS data and supporting systems in accordance with Federal requirements. Specifically, the State had not implemented an adequate risk management process that included contractor oversight, established a security plan for the MMIS, implemented media protection for laptop computers, met Federal requirements for the security of software and data, adequately addressed vulnerabilities on network devices or Web sites, or implemented adequate security awareness and role-based training programs. These weaknesses occurred because the State had not established priorities or allocated the resources necessary to secure Medicaid systems and information.

Although we did not find evidence that anyone had exploited these weaknesses, exploitation could have resulted in unauthorized access to and disclosure of beneficiaries' electronic protected health information, as well as disruption of critical Medicaid operations. The weaknesses were collectively and, in some cases, individually significant and could have compromised the integrity of the State's Medicaid program.

WHAT WE RECOMMENDED

We recommended that the State establish priorities and allocate the resources necessary to implement our detailed recommendations for improving the controls necessary to safeguard its Medicaid information and systems. We communicated with the State our findings on control weaknesses throughout the audit and before we issued our draft report. Because of the sensitive nature of our findings, we have not listed the detailed recommendations in this summary.

STATE COMMENTS

In written comments on our draft report, the State concurred with all of our recommendations and described actions that it had taken or planned to take to implement them.