Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PUBLIC SUMMARY REPORT: INFORMATION TECHNOLOGY CONTROL WEAKNESSES FOUND AT THE COMMONWEALTH OF MASSACHUSETTS' MEDICAID MANAGEMENT INFORMATION SYSTEM

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

March 2017
A-06-15-00057

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 8L 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.

Massachusetts did not ensure that it adequately protected its Medicaid data and information systems to reduce vulnerabilities that could have potentially compromised the integrity of the Medicaid program.

This summary report provides an overview of the results of our audit of the information security controls at Massachusetts's Executive Office of Health and Human Services, which is responsible for administering the State Medicaid program (MassHealth). 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 MassHealth 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.

The Massachusetts Executive Office of Health and Human Services is responsible for administering MassHealth. MassHealth has service-level agreements with the Massachusetts Office of Information Technology to maintain, support, and provide information technology (IT) architecture services. MassHealth contracts with Hewlett-Packard for application support. The Medicaid Management Information System (MMIS) mainly supports Medicaid claims processing, recovery of claims' reimbursement from third parties, managed care, the provider self-service portal, and health care authorization services. The MMIS supports more than 1.67 million beneficiaries, and processed approximately $13.8 billion in fiscal year 2015.

The objective of our review was to determine whether Massachusetts safeguarded MMIS data and supporting systems in accordance with Federal requirements.

HOW WE CONDUCTED THIS REVIEW

We focused our audit on MassHealth's Web sites, databases, and other supporting information systems. We reviewed MassHealth's implementation of Federal requirements and National Institute of Standards and Technology guidelines within the following areas: system security plan, risk assessment, data encryption, Web applications, vulnerability management, and database applications. We limited our review to these security control areas and to controls that were in place at the time of our site visit. We did not review MassHealth's internal controls.

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 provides a reasonable basis for our findings and conclusions based on our audit objectives. We communicated to MassHealth our preliminary findings in advance of issuing our draft report.

WHAT WE FOUND

MassHealth did not safeguard MMIS data and supporting systems in accordance with Federal requirements. Specifically, MassHealth had vulnerabilities related to security management, configuration management, system software controls, and Web site and database vulnerability scans.

Although we did not identify evidence that the vulnerabilities had been exploited, exploitation could have resulted in unauthorized access to, and disclosure of, sensitive information, as well as disruption of operations critical to MassHealth. As a result, the vulnerabilities were collectively and, in some cases, individually significant and could have potentially compromised the confidentiality, integrity, and availability of MassHealth's MMIS. These vulnerabilities existed because MassHealth did not implement sufficient controls over its Medicaid data and information systems.

WHAT WE RECOMMENDED

We recommended that MassHealth implement our detailed recommendations to address the findings that we identified related to security management, configuration management, system software controls, and Web site and database vulnerability scans.

AUDITEE COMMENTS

In written comments on our draft report, MassHealth did not explicitly express concurrence or noncurrence with our eight recommendations; however, it described corrective actions that it had taken or planned to take to remediate all the vulnerabilities. MassHealth questioned the number of computers associated with one finding. MassHealth did not provide supporting documentation to dispute our analysis.