Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PUBLIC SUMMARY REPORT: INFORMATION TECHNOLOGY CONTROL WEAKNESSES FOUND AT THE MINNESOTA HEALTH INSURANCE EXCHANGE

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

Amy J. Frontz
Assistant Inspector General
for Audit Services

September 2016
A-06-15-00035

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.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at http://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.

Minnesota implemented security controls over the Web site, database, and other supporting information systems for its health insurance exchange. However, improvements are needed to fully comply with Federal and State requirements and to increase protection of personally identifiable information.

This summary report provides an overview of the results of our audit of the information security controls at Minnesota's Health Insurance Marketplace (MNsure). It does not include specific details of the vulnerabilities that were identified because of the sensitive nature of the information. We provided more detailed information and recommendations to MNsure so that it could 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 Patient Protection and Affordable Care Act (ACA)[1] established health insurance exchanges (commonly referred to as "marketplaces") to allow individuals and small businesses to shop for health insurance in all 50 States and the District of Columbia. Because the marketplaces handle consumers' personally identifiable information (PII), security of the marketplaces' data and systems is paramount. Web applications (Web sites) and database systems that are not properly secured create vulnerabilities that could be exploited by unauthorized persons to compromise the confidentiality of PII. One of the top challenges in the U.S. Department of Health and Human Services, Office of Inspector General's list of management challenges facing the Department is ensuring the security of the marketplaces. The review summarized here is one of a series of reviews of State-based marketplaces' security controls.

Under provisions of the ACA, Minnesota chose to implement a State-based marketplace. Minnesotans may use the MNsure Web site to shop for, compare, and choose health insurance coverage that meets their needs. MNsure is the only place where Minnesota residents can qualify for financial help through Federal tax credits or through MinnesotaCare and Medical Assistance. The Minnesota Information Technology Agency operates and manages the MNsure Web site.

Our objective was to determine whether MNsure had implemented security controls to protect PII on its Web site, database, and other supporting information systems in accordance with Federal and State requirements.

HOW WE CONDUCTED THIS REVIEW

We focused our audit on MNsure's Web site, database, and other supporting information systems. Our review of applicable Federal requirements included reviewing (1) Centers for Medicare & Medicaid Services' *Minimum Acceptable Risk Standards for Exchanges* Document

[1]P.L. No. 111-148 (Mar. 23, 2010), as amended by the Health Care and Education Reconciliation Act of 2010, P.L. No. 111-152 (Mar. 30, 2010).

Suite[2] and (2) National Institute of Standards and Technology guidelines on the following: system security plan, risk assessment, data encryption, Web applications, vulnerability management, plan of action and milestones, and database applications. We also reviewed the Minnesota Office of Enterprise Technology's *Enterprise Vulnerability Management Security Standard*. We did not review MNsure's overall internal controls. We conducted our fieldwork at MNsure offices in Minneapolis, Minnesota, in July 2015.

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.

WHAT WE FOUND

MNsure had implemented security controls, policies, and procedures intended to prevent vulnerabilities in its Web site, database, and other supporting information systems. However, it did not always comply with Federal and State information technology requirements when it implemented those security controls, policies, and procedures, which increased MNsure's risk that PII could have been exposed. Specifically, MNsure had not formalized procedures for analyzing and sharing information about vulnerabilities and had vulnerabilities related to penetration testing and Web site monitoring procedures. Additionally, our Web site and database vulnerability scans identified numerous weaknesses.

Although we did not identify evidence that the vulnerabilities had been exploited, exploitation could have resulted in unauthorized access to and disclosure of PII, as well as disruption of critical marketplace operations. The vulnerabilities were collectively and, in some cases, individually significant and could have potentially compromised the integrity of the marketplace. In addition, without properly implemented policies and procedures, systems were not protected from individuals and groups with malicious intent to obtain access to commit fraud, waste, or abuse or to launch attacks against other computer systems and networks.

We promptly shared detailed information with MNsure on preliminary findings in advance of issuing our draft report.

WHAT WE RECOMMENDED

We recommended that MNsure implement our four detailed recommendations to address the findings that we identified. Because of the sensitive nature of our findings, we have not listed the detailed recommendations in this summary report.

[2]The Document Suite (Aug. 1, 2012) includes *Minimum Acceptable Risk Standards for Exchanges—Exchange Reference Architecture Supplement, Catalog of Minimum Acceptable Risk Controls for Exchanges—Exchange Reference Architecture Supplement*, and *ACA System Security Plan Procedures.*

MINNESOTA HEALTH INSURANCE MARKETPLACE COMMENTS AND OUR RESPONSE

In written comments on our draft report, MNsure concurred with one of our four recommendations, partially concurred with one recommendation, and did not concur with two recommendations. MNsure described actions that it has taken or plans to take to implement our recommendations.

We maintain that our findings and recommendations are valid.