Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

PUBLIC SUMMARY REPORT: NEW YORK IMPLEMENTED SECURITY CONTROLS OVER ITS HEALTH EXCHANGE WEB SITE AND DATABASE BUT COULD IMPROVE SECURITY CONTROLS

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

November 2016
A-02-15-03001

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 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.

New York implemented security controls over the Web site and database for its health insurance exchange. However, improvements are needed to fully comply with Federal 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 New York's health insurance exchange, New York State of Health (New York marketplace). 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 New York marketplace 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 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 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 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, New York chose to implement a State-based marketplace. The Federal Government awarded New York $571 million to support the marketplace's development. The New York's NY State of Health Web site offers State residents side-by-side comparisons of qualified health plans; tax credits or financial help to pay for health insurance premiums and copayments; and online customer support. The New York marketplace uses an IBM DB2 database to store PII. As of January 2, 2016, the New York marketplace had received more than 10.9 million unique applications for the individual market and more than 11,000 applications from employers.

Our objective was to determine whether the New York marketplace had implemented security controls to protect PII on its Web site and database in accordance with Federal requirements.

HOW WE CONDUCTED THIS REVIEW

We reviewed the New York marketplace's information security controls, including its policies and procedures, in place at the time our fieldwork began in March 2016. Our review of applicable Federal requirements included reviewing certain Centers for Medicare & Medicaid Services (CMS) requirements in the *Minimum Acceptable Risk Standards for Exchanges*

[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).

Document Suite.[2] These requirements and standards include those related to security plans and risk assessments, vulnerability scanning and penetration testing, patch management and flaw remediation, Plan of Action and Milestones,[3] and incident response. We did not review the New York marketplace's overall 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 provided a reasonable basis for our findings and conclusions based on our audit objectives. We communicated to the New York marketplace our preliminary findings in advance of issuing our draft report.

WHAT WE FOUND

The New York marketplace had implemented many security controls, including policies and procedures, to protect PII on its Web site and database. However, it did not always comply with Federal requirements. Specifically, the New York marketplace had not adequately secured its Web site.

Although we did not identify evidence that the vulnerabilities in the New York marketplace's Web site had been exploited, exploitation could have resulted in unauthorized access to and disclosure of PII, as well as disruption of critical marketplace operations. As a result, the vulnerabilities were collectively and, in some cases, individually significant and could have potentially compromised the confidentiality, integrity, and availability of the marketplace. In addition, without proper safeguards, systems were not protected from individuals and groups with malicious intent to obtain access in order to commit fraud, waste, or abuse or launch attacks against other computer systems and networks.

WHAT WE RECOMMENDED

We recommended that the New York marketplace improve the protection of PII on its Web site in accordance with Federal requirements by adequately securing its Web site. Because of the sensitive nature of our findings, we have not listed the detailed findings in this summary report.

NEW YORK MARKETPLACE COMMENTS

In written comments on our draft report, the New York marketplace did not indicate concurrence or nonconcurrence with our recommendation or the specific vulnerabilities identified. The New

[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*.

[3] Organizations, including the New York marketplace, use the Plan of Action and Milestones to report to CMS their planned remedial actions to correct vulnerabilities identified during security assessments.

York marketplace disagreed with one of the findings and in some instances disagreed with the scanning tool's assignment of the risk level because the New York marketplace determined that the findings did not pose any risk to the protection of PII.

After reviewing the New York marketplace's comments, we maintain that our findings and assessment of associated risk are valid.