Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PUBLIC SUMMARY REPORT: CONNECT FOR HEALTH COLORADO GENERALLY PROTECTED PERSONALLY IDENTIFIABLE INFORMATION ON ITS HEALTH INSURANCE EXCHANGE WEB SITES AND DATABASES BUT COULD CONTINUE TO IMPROVE INFORMATION SECURITY CONTROLS

Inquiries 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-07-15-00454

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.

Colorado implemented security controls over the Web sites and databases for its health insurance exchange. However, improvements are still needed to fully comply with Federal requirements and to increase protection of personally identifiable information.

This public summary report provides an overview of the results of our audit of the information security controls at Colorado's health insurance exchange, Connect for Health Colorado (C4HCO). 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 C4CHO so that it can address the issues we identified. The findings listed in this public 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. In the U.S. Department of Health and Human Services, Office of Inspector General's annual list of management challenges facing the Department, protecting and ensuring the confidentiality and integrity of consumers' sensitive personal information and marketplace information is currently one of the top challenges. The review summarized here is one of a series of reviews of State-based marketplaces.

In 2011, the Colorado General Assembly passed Senate Bill 11-200, which created the Colorado Health Benefit Exchange (COHBE) as a public, nonprofit entity responsible for operating the State-based marketplace. Doing business as C4HCO, its mission is to increase access, affordability, and choice for individuals and small businesses purchasing health insurance in Colorado. Under provisions of the ACA, Colorado applied for and received four grant awards totaling more than $184 million to create and implement its health insurance marketplace. C4HCO contracted with CGI Technologies and Solutions, Inc. (CGI), as the systems integrator for the COHBE system.

The objective of our review was to determine whether C4HCO had implemented security controls to protect PII on its COHBE Web sites and databases in accordance with Federal requirements.

HOW WE CONDUCTED THIS REVIEW

We reviewed C4HCO's information security controls in place as of November 2014, including its system security plan, risk assessments, supporting policies and procedures, and capabilities

[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), collectively referred to as "ACA."

for identifying vulnerabilities. We limited our review to C4HCO's implementation of certain controls over the security of its COHBE Web sites and databases.
Our review of applicable Federal requirements included reviewing certain Centers for Medicare & Medicaid requirements in the *Minimum Acceptable Risk Standards for Exchanges* Document Suite.[2] We did not review C4HCO's overall internal controls. We performed our onsite fieldwork at the CGI offices in Denver, Colorado, in November 2014.

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

C4HCO had implemented many security controls on its COHBE Web sites and databases with the intent to protect PII; however, it did not fully comply with Federal requirements, which increased C4HCO's risk that PII could have been exposed. Specifically, C4HCO had not updated the system security plan's supporting policies or ensured that vulnerabilities identified during prior scans were mitigated in a timely manner. Additionally, our database security scans identified numerous weaknesses regarding user access administration and inadequate security settings. Moreover, C4HCO had not performed incident response testing.

Although we did not find evidence that the weaknesses 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 weaknesses were collectively and, in some cases, individually significant and could have compromised the integrity of Colorado's marketplace, thus increasing the risk that PII could have been exposed. In addition, without proper safeguards, systems are not protected from individuals and groups that obtain access to commit fraud, waste, or abuse or launch attacks against other computer systems and networks.

WHAT WE RECOMMENDED

We recommended that C4HCO implement our detailed recommendations to address the findings that we identified related to the COHBE system security plan, vulnerability mitigation, database user access administration and security settings, and incident response capability.

CONNECT FOR HEALTH COLORADO COMMENTS AND CORRECTIVE ACTION EFFORTS

In written comments on our draft report, C4HCO concurred with our recommendations and described corrective actions that it had taken or planned to take.

[2] The Document Suite 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.*

After we had scanned C4HCO's application production databases during our fieldwork but before we issued our draft report, we shared information with C4HCO officials on the vulnerabilities we had identified and on our preliminary findings. C4HCO, working in conjunction with CGI, began remediation efforts before we completed our fieldwork.

After we issued our final report but before we published this public summary report, C4HCO gave us evidence to support its remediation efforts. Although we have not conducted additional onsite fieldwork, we have reviewed the evidence of remediation. Based on the evidence provided, C4HCO has successfully remediated the issues we found related to the system security plan and incident response testing and has partially remediated the issues we found related to the application production databases and vulnerability mitigation.