# HHS OIG Hackers Test Health Insurance Exchange Websites

Posted At : September 30, 2014 9:15 AM | Posted By : Angie Petty
Related Categories: Health IT, Health and Human Services, Health Care

HHS Office of Inspector General (OIG) auditors conducted audits of Healthcare.gov, the Kentucky Health Benefit Exchange, and the New Mexico Health Insurance Exchange during February through June 2014, to include vulnerability scans and simulated attacks.

Auditors praised each marketplace for aspects of their security controls, policies, procedures and testing, while making recommendations for improvements in areas where they spotted vulnerabilities.

Findings and recommendations for each marketplace are specified below:

**Healthcare.gov**

CMS has taken actions in the last year to lower the security risks associated with Healthcare.gov systems and consumer Personal Identifying Information (PII), including:

- Establishing a dedicated security team under the CIO to monitor and track corrective action plans for vulnerabilities and ensure they are completed
- Performing weekly vulnerability scans
- Completing two security control assessments

Suggested areas for improvement are as follows:

- Implement a process to use automated tools to test database security configuration settings on all databases
- Implement an effective enterprise scanning tool to test for web site vulnerabilities
- Maintain adequate documentation to verify that database property files containing user credentials have been closed by encrypting the file
- Detect and defend against web site vulnerability scanning and simulated cyber attacks directed at the Healthcare.gov web site
- Finish corrective action already underway to remedy a critical vulnerability. The publically available OIG summary did not convey specifics of this vulnerability. However, CMS stated that their scheduled completion date for corrective action was June 30, 2014.

**Kentucky Health Benefit Exchange (KHBE)**

According to the HHS OIG, the KHBE had sufficiently protected PII in accordance with federal requirements. Using encryption, Kentucky properly secured individual’s PII upon system entry, as well as during storage and transmission. However, the OIG identified the following areas of opportunity for improvement for database access and security control:

- Sufficiently restrict user and group access to authorized roles and functions
- Address federal requirements for system security planning, risk assessment, penetration testing and flaw remediation, POA&M, and incident response capability

The above deficiencies were mainly due to the fact that Kentucky was transitioning its information technology responsibilities among agencies and had not sufficiently established coordination between them, to date.

**New Mexico Health Insurance Exchange (NMHIX)**

The HHS OIG found that the NMHIX had implemented security controls, policies, and procedures to prevent vulnerabilities in its website, database, and supporting information systems. However, NMHIX’s IT policies and procedures did not always conform to federal IT requirements and NIST recommendations.

Specifically, the audit identified the following vulnerabilities:

- One data encryption vulnerability
- Two remote access vulnerabilities
- One patch management vulnerability
- One Universal Serial Bus port and device vulnerability

- 64 web application vulnerabilities, two of which were listed as critical
- 74 data base vulnerabilities, one of which were listed as high

In written responses to the HHS OIG, all of the exchanges concurred with most of the findings and recommendations and furnished plans regarding how they planned to address vulnerabilities cited.